المسئولية الجنائية
لانتهاك الخصوصية المعلوماتية
دراسة مقارنة



المسئولية الجنائية

لانتهاك الخصوصية المعلوماتية

المسئولية الجنائية

لانتهاك الخصوصية المعلوماتية

الدكتور

محمد نصر محمد

الطبعة الأولى

1436 هـ - 2015 م



رقم الإيداع

2015/23445


ISBN 978-977-6504-07-3

مركز الدراسات العربية
للنشر والتوزيع

طريقك إلى المعرفة

جمهورية مصر العربية

الجيزة - 6 أكتوبر - الحي الخامس - ش 13
002 (02) 383 767 64
002 010 440 490 6
00966 543 044 662
www.ascpublishing.com
info@ascpublishing.com
markez.derasat@gmail.com

بسم الله الرحمن الرحيم

مقدمة

مُنذ بدايات القرن الجديد ومع تزايد الإهتمام بالمعلوماتية، حتي أطلق علي العصر الراهن (بالعصر الرقمي)، ثار الجدل حول المركز القانوني لمتعهدى الإيواء(مقدمي خدمات الإنترنت)، ودورهم في الوصول الأمثل لاستخدام الشبكة، وبخاصة أنهم المنوط بهم إما فتح نطاقات علي شبكة المعلومات، أو مقدمي خدمات معلوماتية من خلال الشبكة، أو خالقين بيئة للتواصل الإجتماعي، وتذرَّع مقدمو الخدمات كثيراً من أجل التخفيف من الالتزامات التي ألقاها القضاء- في بداياته- على عاتقهم، وضغطوا، في نفس الوقت، لإرساء نظامٍ خاصٍّ يُعفيهم من المسؤولية، سواء عن إخلالهم بتقديم الخدمة أو عن عدم مشروعيَّة المضمون المعلوماتي المتداول عبر أجهزتهم، الأمر الذي أثار الكثير من الإشكاليات القانونية والفنية، تدخَّلت التشريعات المعاصرة، كالتشريعين الأُوروبي والفرنسي، لحسم الجدل، ولوضعِ نظامٍ قانونيٍّ خاصٍّ بمقدمي خدمات الإنترنت، فحدَّدت، من خلاله بدقَّة، الالتزامات الملقاة على عاتقهم، والأحكام الخاصة بمسؤوليتهم عمَّا يحدث من مخالفات عبر الشبكة[1].

(1) Vacca، John. (1996). Internet Security Secrets.USA:IDG Book. Worldwide Inc.Wilson، c. (2000) Holding management accountable: a new policy for protect against computer crime. Proceedings of the National Aerospace and Electronics Conference، USA 2000، 272281-.

ولا شك ان البلدان العربية، أضحت هدفا، كما ان تأثيرات تلك الأفعال غير المشروعة فاقت كل التصورات، كما كان لها أكبر الأثر علي منظومة الإقتصاد، فثار التساؤل الهام حول مدى جدوى إعمال القواعد العامة، لإيجاد حلول متوازنة تتفق مع الطبيعة الخاصة لآلية عمل مقدمي خدمات الإنترنت.

أهمية البحث:

مع التقدم التكنولوجي الهائل، وتقدم تقنية الإتصالات، واكب ذلك زيادة تغيرات في نشاطات العناصر الإجرامية، ولكن هناك تشابه بين الجريمة الالكترونية مع الجريمة التقليدية فى أطراف الجريمة من مجرم ذي دافع لارتكاب الجريمة و ضحية و الذي قد يكون شخص طبيعي أو شخص اعتباري وأداة ومكان الجريمة، وهنا يكمن الاختلاف الحقيقي بين نوعى الجريمة ففي الجريمة الالكترونية الأداة ذات تقنية عالية وأيضا مكان الجريمة الذي لا يتطلب انتقال الجاني إليه انتقالا ماديا(إستاتيكيا) و لكن فى الكثير من تلك الجرائم فان الجريمة تتم عن بعد باستخدام خطوط و شبكات الاتصال بين الجاني ومكان الجريمة، كما أن أدلة ثبوتها تحتاج إلي تحليل خاص، كما أنها تتميز بسهولة إخفاء معالمها.

هذا وتشير مجلة لوس انجلوس تايمز فى عددها الصادر فى 22 مارس عام 2000 إلى أن خسارة الشركات الاميريكية وحدها من جراء الممارسات التى تتعرض لها والتى تندرج تحت بند الجريمة الالكترونية بحوالى 10 مليار دولار سنويا، و للتأكيد على جانب قد تغفله الكثير من مؤسسات الأعمال فان نسبة 62% من تلك الجرائم تحدث من خارج المؤسسة و عن طريق شبكة الانترنت بينما تشكل النسبة الباقية (38 %) من تلك الخسائر من ممارسات تحدث من داخل المؤسسات ذاتها.

مثال آخر: حديث قد لا يتوقع أحدكم الخسائر الناجمة عنه وهو تلك الأعطال والخسائر فى البرامج والتطبيقات والملفات ونظم العمل الآلية وسرعة وكفاءة شبكات الاتصال والذى ينجم عن التعرض للفيروسات والديدان مثل ذلك الهجوم الأخير والذى تعرضت له الحواسب الآلية المتصلة بشبكة الانترنت فى اغلب دول العالم من خلال فيروس يدعى (WS32.SOBIG) والذى أصاب تلك الأجهزة من خلال رسائل البريد الالكتروني بصورة ذكية للغاية حيث كان ذلك الفيروس يتخفى فى الوثيقة الملحقة بالبريد الالكتروني (Attachment File) فى صورة ملف ذو اسم براق و عند محاولة فتح ذلك الملف فان الفيروس ينشط ويصيب جهاز الحاسب و يبدأ فى إرسال المئات من رسائل البريد الالكتروني من ذلك الجهاز المصاب مستخدما كل أسماء حسابات البريد الالكتروني المخزنة عليه، الأمر الذي أدى إلى إصابة عدد هائل من الحواسب الشخصية للأفراد و الشركات و ملء خوادم البريد الالكتروني بتلك الرسائل مثال على ذلك: إصابة خوادم البريد الالكتروني لشركة أميركا اون لاين بما يقارب ال 20مليون رسالة ملوثة وأدى ذلك أيضا إلى بطء شبكات و خطوط الاتصال[1] بصورة كبيرة وأحيانا بالشلل التام مما أدى لتعطل الكثير من الأعمال و تلف العديد من الملفات الهامة على تلك الحواسب وقد قدرت الخسائر الناجمة عن ذلك الفيروس بما يقارب الـ 50مليون دولار اميريكى فى داخل الولايات المتحدة الاميريكية وحدها[2].

ومن الجرائم الأخرى ذات التأثيرات المختلفة سرقة بيانات بطاقات الائتمان الشخصية والدخول على الحسابات البنكية وتعديلها وسرقة الأسرار

(1) ويمكنك ملاحظة وجود الفيروس في جهازك إذا ما كان الحاسب الآلي يحتاج لوقت أكثر من اللازم لتحميل أو تنفيذ البرامج، أو تغيّر في حجم الذاكرة، أو اختفاء بعض الملفات، أو ظهور رسائل غير اعتيادية على الشاشة، أو وجود إشارات غير عادية أو أصوات غير عادية تطلق من جهاز الحاسوب وقد تكون هذه الإشارات لأسباب أخرى غير الفيروسات.

(2) H. Feraud، E. Schlanilz، la cooperatation policiere international، R.I.D. P، 1974، p477478-

الشخصية والعملية الموجودة بصورة الكترونية وأيضا الدخول على المواقع وقواعد البيانات وتغيير أو سرقة [1]محتوياتها وأيضا بث الأفكار الهدامة أو المضادة لجماعات أو حكومات بعينها وأيضا السب والقذف والتشهير بالشخصيات العادية والعامة ورموز الدين والسياسة وخلافه.

وبالنظر في نطاق القانون الجنائي، يعرف إتجاه في الفقه[2] الجريمة"بأنها فعل غير مشروع صادر عن إرادة جنائية يقرر لها القانون عقوبة أو تدبيراً احترازياً".

أما بالنسبة لجرائم الكمبيوتر (الحواسيب) والانترنت، فقد تعددت التعريفات وفقا لمعايير متعددة سواء أكانت وفقا لمعيار شخصي من حيث توفر المعرفة والدراية بالتقنية أو وفقا لمعيار موضوع الجريمة، والمعايير المتعلقة بالبيئة المرتكب فيها الجريمة، وغيرها.

ونلاحظ أن هذه الجرائم كانت تستهدف أنظمة بعينها، وصحيح أن ذلك يتم من خلال بيئة الشبكة المعلوماتية ككل، ولكن ما نرمي إليه بشكل جزئي لتحديد المسؤولية الجنائية للوسطاء ومقدمي الخدمة، قاصرين ذلك

---

(1) قد يقوم الفيروس بحذف الجزء الأول من الملف التنفيذي وكتابة نفسه في هذا المكان، الأمر الذي يؤدي إلي توقف عمل هذا الملف بشكل جزئي ويعرف هذا النوع من الفيروسات باسم فيروسات الكتابة الفوقية، وقد يقوم الفيروس بنسخ نفسه في الجزء الأخير من الملف التنفيذي ويعرف هذا النوع من الفيروسات باسم فيروسات الكتابة غير الفوقية. وهناك فيروس الكتابة المباشرة حيث يقوم بكتابة نفسه مباشرة على الأسطوانة الصلبة في مكان محدد،فيؤدي إلي عدم قدرة نظام التشغيل على التعامل مع الملفات بالرغم من أن هذه الملفات مازالت موجودة علي القرص الصلب ولم يتم حذفها ومن أشهر هذه الفيروسات فيروس تشرنوبل. ولقد ظهرت هذه النوعية من البرامج الضارة لأول مرة في عام 1988 على يد الطالب الأمريكي Roper Tappan Morris وهي ما عرفت بدودة موريس Morris، ومن أشهرها دودة الحب"Love Bug"والتي ظهرت عام 2000م وتسببت في خسائر تقدر بملاين الدولارات، راجع مقال جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت- المرجع السابق.

(2) د. محمد بوشيبة"حماية برامج الحاسوب طبقا لقانون 000 2 المنظم لحقوق المؤلف والحقوق المجاورة"مجلة القضاء والقانون، عدد. ص. 84.

علي النطاق المعلوماتي الخاص بكل منهم، حتي نصل إلي إيجاد مرجعية عامة للشبكة المعلوماتية ككل.

وسنعرض لموقف الفقه الجنائي من تحديد لماهية العمل الغير المشروع والذي يتخذ البيئة المعلوماتية لتحقيق أهدافه.

فقد عرفتها الدكتورة هدي قشقوش بأنها:"كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"[1].

وعرفها الأستاذ Rosenblatt بأنها"كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلي المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه".

كما عرفها الفقيه ArtarSolarz بأنها"أي نمط من أنماط الجرائم المعروف في قانون العقوبات طالما كان مرتبط بتقنية المعلومات".

كذلك عرفها الأستاذ EslieD.Ball بأنها"فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية".

كما عرفتها وزارة العدل الأمريكية بأنها"أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها"[2].

ويعرفها Sheldon بأنها"واقعة تتضمن تقنية الحاسب ومجني عليه يتكبد أو يمكن أن يتكبد خسارة وفاعل يحصل عن عمد أو يمكنه الحصول علي مكسب".

---

(1) د. محمد حسين منصور- المسئولية الالكترونية- دار الجامعة الجديدة للنشر الإسكندرية- طبعة 2003- صفحة 294.

(2) Philippe JOUGLEDX، droit des médias، faculté de droit d'aix- Marseille، dans le thème :"la criminalité dans le cuber- espace »، 1999، p : 25 et suivants.

كـما يعرفهـا خـبراء منظمـة التعـاون الاقتصـادي والتنميـة OECD بأنهـا"كل سـلوك غـير مـشروع أو غـير أخلاقـي أو غـير مـصرح بـه يتعلـق بالمعالجـة الآليـة للبيانــات أو نقلهــا".

ويعرفهـا الفقيــه الفرنــسي Vivant بأنها"مجموعــة مــن الأفعــال المرتبطــة بالمعلوماتيــة والتــي يمكــن أن تكــون جديــرة بالعقــاب [1]

كـما يعرفهـا الأسـتاذين Robert J.Lindquist، Jack Bologna بأنها"جريمـة يسـتخدم فيهـا الحاسـوب كوسـيلة أو أداة لارتكابهـا أو يمثـل إغـراء بذلـك أو جريمـة يكـون الكمبيوتـر نفسـه ضحيتهـا.

أنـواع الجريمة الالكترونية:

أولا الجرائـم التى تتم ضد الحواسـب الآليـة ونظم المعلومات[2]

1 -جرائـم الإضرار بالبيانات:

يعتــبر هــذا الفــرع مــن الجرائــم الالكترونيــة مــن أشــدها خطــورة و تأثــيرا وأكثرهــا حدوثــا وتحقيقــاُ للخســائر للأفــراد والمؤسســات، ويشــمل هــذا الفــرع كل أنشــطة تعديــل أو محــو أو سرقــة أو إتــلاف أو تعطيــل العمــل للمعلومــات وقواعــد البيانـات الموجـودة بصـورة الكترونيـة (Digital Form) عـلى الحواسـب الآليـة المتصلـة بشــبكات المعلومــات أو مجــرد محاولــة الدخــول بطريقــة غــير مشروعــة عليهــا.

(1) في هذا الإطار فقد قام أحد المسؤولين الإعلاميين بإحدى الشركات بعد فصله عن العمل بزرع قنبلة منطقية زمنية في برنامج الشركة أدى إلى انهيار النظام كاملا لمدة شهر كامل مما كبد الشركة خسائر كبيرة. أنظر بهذا العدد: Mohammed Bozobar أنظر المقال السابق ص: 523.

(2) Nanoart.(2000) [Online]. Available: http://www.nanoart.f2s.com/hack/ [15.11.2000] NUA Internet Surveys. (1998،June). How Many Online? [Online].Available: http: // www. nua. ie/ surveys/ howmayonline/ index. html [26. 10.2000].

أبسـط تلـك الأنشـطة هـو الدخـول لأنظمـة المعلومـات وقواعـد البيانـات بصـورة غـير مشروعـة والخـروج دون إحـداث أى تأثـير سـلبي عليهـا[1]، ويقـوم بذلـك النـوع مـن الأنشـطة مـا يطلـق عليهـم المخترقـون ذوى القبعـات البيضـاء[2] (White Hat Hackers) الذيـن يقومـون بالدخـول بطريقـة غـير مشروعـة عـلى أنظمـة الحاسـب أو شـبكات المعلومـات أو مواقـع الانترنـت مسـتغلين بعـض الثغـرات فى تلـك النظـم مخترقـين بذلـك كل سياسـات و إجـراءات امـن المعلومـات التـى يقـوم بهـا مديـري تلـك الأنظمـة والشـبكات (System And Network Administrators) ونتيجـة عـدم ارتبـاط ذلـك النشـاط بالشـبكات فاخـتراق الأمـن بطريـق مـادي للاماكـن التـى يوجـد بهـا أجهـزة الحاسـب التـى تحتـوى عـلى بيانـات هامـة بالرغـم مـن وجـود إجـراءات أمنيـة لمنـع الوصـول إليهـا و بمعنـى آخـر وصـول شـخص غـير مـصرح لـه و إمكانيـة دخولـه إلى حجـرة الحواسـب المركزيـة بالمؤسسـة ثـم خروجـه دون إحـداث أى أضرار فانـه يعتـبر خـرق السياسـة وإجـراءات امـن المعلومـات بتلـك المؤسسـة، ولا تعـد الأخـيرة تمثـل صعوبـة في التحقـق منهـا[3].

---

(1) وتجرم بعض التشريعات العربية حتي مجرد الإستخدام دون تحقيق أية غاية نفعية طالما تحقق الضرر حتي ولو كان محتملا»الشاب مرتضى (...) حكم بثلاث سنوات سجنا نافذا وغرامة 10.000 درهما (حوالي 970 يورو) بتهمة انتحال صفة بعد انخراطه في موقع"فايس بوك"ببروفايل سماه"الأمير مولاي رشيد"بدون أية غاية نفعية أو إجرامية ودون حتى إرسال أية رسالة منه. ونطق الحكم من طرف المحكمة الابتدائية بالدار البيضاء مساء يوم الجمعة 22 فبراير 2008 في محاكمة غابت فيها كل شروط وضمانات المحاكمة العادلة»، يقول بلاغ الجمعية،من جهتها، أنشأت أسرة فؤاد موقعا على الانترنيت خاصا بالتضامن معه، زوار الموقع تجاوز عددهم 71 ألف شخص خلال أقل من ثلاث أسابيع، كما بلغ عدد التوقيعات على العريضة التضامنية 7000 توقيع. في نفس الوقت، أنشأ عدد من مستعملي"فايس بوك"صفحة تضامنية مع فؤاد بلغ عدد أعضائها 4000 شخص، فيما وضع العشرات من مستعملي"فايس بوك"صورة فؤاد بدل صورتهم على صفحاتهم الخاصة في الموقع.

(2) برنامج (Back Orific): ثاني أشهر البرامج وأقدمها يعطي المستخدم قدرة كاملة على جهاز الضحية تم الإعلان عنه من قبل جهة تدعـى بجمعية البقرة الميتة (Cult of Dead Cow) والإصدارة التي صدرت في عام 1999 باسم بـ (BO2K)

(3) Bouchaib RMAIL، la criminalité informatique، criminalité a double dimension :internationale، thèse pour l'obtention du grade de ducteur en droit privé- option : droit des affaires، faculté des sciences juridiques، économiques et sociales- fés، 2005، p : 82.

استخدام الشبكات و بصفة خاصة شبكة الانترنت فى الدخول على قواعد البيانات أو مواقع الانترنت والحصول على معلومات غير مسموح بها أو إمكانية السيطرة التامة على تلك الأنظمة بالرغم من وجود إجراءات حماية متعددة الدرجات من الحوائط النارية وأنظمة كشف ومنع الاختراق بالإضافة لآليات تشفير البيانات وكلمات السر المعقدة وبتخطي كل تلك الحواجز والدخول على الأنظمة المعلومات ثم الخروج دون إحداث أى تغيير أو إتلاف بها فانه ابسط أنواع الاختراق الذي يعطى الإشارة الحمراء لمديري النظم وأمن المعلومات بان سياساتهم وإجراءاتهم التنفيذية لأمن المعلومات بحاجة إلى التعديل والتغيير وانه يتعين عليهم البدء مرة أخرى فى عمل اختبار وتحليل للتهديدات ونقاط الضعف الموجودة بأنظمتهم (Risk Assessment) لإعادة بناء النظام الامنى مرة أخرى وأيضا العمل على إجراء ذلك الاختبار بصورة دورية لمواكبة الأساليب الجديدة فى الاختراق.

أما بالنسبة الى تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل لنظم المعلومات فان تلك الأنشطة تتم بواسطة أفراد هواه أومحترفون يطلق عليهم المخترقون ذوى القبعات السوداء (Black Hat Hackers) الذين قد يقومون بهذه الأعمال بغرض الاستفادة المادية أو المعنوية من البيانات والمعلومات التى يقومون بالاستيلاء عليها أو بغرض الإضرار بالجهة صاحبة تلك الأنظمة لوجود كره شخصي أو قبلي أو سياسي أو ديني أو القيام بذلك لحساب احد المؤسسات المنافسة.

مثال على ذلك: ما ذكره مكتب التحقيقات الفيدرالية الاميريكى (FBI) فى السادس و العشرون من سبتمبر عام 2002 من القبض على احد عملائها و يدعى ماريوكاستللو 36 عاما ومحاكمته بتهمة تخطى الحاجز

الامنى المسموح له به و الدخول على احد أجهزة المكتب ستة مرات بغرض الحصول على بعض الأموال[1].

فى التقرير السنوي الثامن لمكتب التحقيقات الفيدرالية الاميريكى الصادر عام 2003 بعنوان جرائم الحاسب فان أكثر خسائر المؤسسات بالولايات المتحدة الاميريكية تأتى من الاستيلاء على المعلومات والتي تكبدتها خلال هذا العام خسائر تتعدى السبعين مليون دولار اميريكى و يأتي فى المركز الثاني نشاط تعطيل نظم المعلومات محققا خسائر تتجاوز الخمسة و ستين و نصف مليون دولار[2].

تعطيل العمل و الذي يطلق عليه ال (Denial Of Service Attack) و اختصاراً ال (Dos) والذي يعتمد على إغراق أجهزة الخوادم

(1) تركي محمد الوطيان، جرائم الحاسب الآلي: دراسة نفسية تحليلية، هذا المقال موجود على الموقع / www. Minshawi. COM. PDR other/ oteyom

(2) برنامج (Sub Seven): أخطر برامج الاختراق يسمى في منطقة الخليج (الباكدور جي) ويطلق عليه البعض اسم القنبلة. تتركز خطورته في أنه يتميز بمخادعة الشخص الذي يحاول إزالته فهو يعيد تركيب نفسه تلقائيا بعد حذفه ويعتبر أقوى برنامج اختراق للأجهزة الشخصية وفي إصدارته الأخيرة يمكنه أن يخترق سيرفر لقنوات المحادثة(Mirc) كما يمكنه اختراق جهاز أي شخص بمجرد معرفة اسمه في (ICQ)كما يمكنه اختراق مزودات البريد(smtp/pop3) يعتبر الاختراق به صعب نسبيا وذلك لعدم انتشار ملف التجسس الخاص به في أجهزة المستخدمين إلا أنه قائما حاليا على الانتشار بصورة مذهلة ويتوقع أنه بحلول منتصف عام 2001 سوف تكون نسبة الأجهزة المصابة بملف السيرفر الخاص به (40-55 ٪) من مستخدمي الإنترنت حول العالم وهذه نسبة مخيفة جدا إذا تحققت فعلا وهذا البرنامج خطير للغاية فهو يمكن المخترق من السيطرة الكاملة على الجهاز وكأنه جالس على الجهاز الخاص به حيث يحتوي البرنامج على أوامر كثيرة تمكنه من السيطرة علي جهاز الضحية بل يستطيع أحيانا الحصول على أشياء لا يستطيع مستخدم الجهاز نفسه الحصول عليها مثل كلمات المرور فالمخترق من هذا البرنامج يستطيع الحصول على جميع كلمات المرور التي يستخدمها صاحب الجهاز !!! ومن أهم أعراض الإصابة بهذا البرنامج ظهور رسالة"قام هذا البرنامج بأداء عملية غير شرعية"وتظهر هذه الرسالة عند ترك الكمبيوتر بدون تحريك الماوس أو النقر على لوحة المفاتيح حيث يقوم البرنامج بعمل تغييرات في حافظة الشاشة وتظهر هذه الرسائل عادة عندما تقوم بإزالة ادخالات البرنامج في ملف(system.ini) .

بـالاف أو ملايـين طلبـات الحصـول عـلى معلومـات الأمـر الـذي لا تحتملـه قـدرة المكونـات الماديـة (Hardware) أو نظـم قواعـد البيانـات والتطبيقـات والبرامـج موجـودة عـلى تلـك الخـوادم التـى تصـاب بالشـلل التـام لعـدم قدرتهـا عـلى تلبيـة هـذا الكـم الهائـل مـن الطلبـات و التعامـل معهـا، ويحتـاج الأمـر إلى سـاعات عديـدة حتـى يتمكـن مديـري النظـم و الشـبكات للتعـرف عـلى مصـادر الهجـوم و عيـوب النظـم لديهـم و اسـتعادة العمـل بصـورة طبيعيـة، و بالطبـع فـان هـذه السـاعات التـى يكـون فيهـا نظـام المعلومـات متعطـلاً تكبـد المؤسسـة الخسـائر الماديـة الجسـيمة فضـلا عـن تعطيـل مصالـح المتعامليـن مـع تلـك الأنظمـة وفقدانهـم الثقـة فى تلـك المؤسسـة و هـروب العمـلاء منهـا إلى مؤسسـات منافسـة كلـما أمكـن ذلـك.

مـن صـور الاعتـداء الأخـرى التـى تمثـل اعتـداء عـلى الملكيـة الفكريـة للأسـماء مـا يحـدث مـن اعتـداءات عـلى أسـماء مواقـع الانترنـت (Domain Names) حيـث أن القاعـدة العالميـة فى تسـجيل أسـماء النطاقـات (والتـي تتـم أيضـا باسـتخدام بطاقـات الائتـمان مـن خـلال شـبكة الانترنـت) [1]هـى أن التسـجيل بالأسـبقية و ليـس بالأحقيـة (First Come First Served) الأمـر الـذي أحـدث الكثـير مـن المخالفـات التـى يتـم تصعيدهـا إلى القضـاء و بتدخـل مـن منظمـة الايـكان التـى تقـوم بتخصيـص عناويـن وأسـماء المواقـع عـلى شـبكة الانترنـت (Internet Corporation for (ICANN) (Assigned Names and Numbers وذلـك مـن اجـل التنـازل عـن النطـاق للجهـة صاحبـة الحـق مـع توقيـع العقوبـة أو الغرامـة المناسـبة.

يحـدث أيضـا فى تسـجيل النطاقـات عـبر الانترنـت و التـى يتـم تسـجيلها

(1) Rapalus، P.(2000،May). Ninety percent of survey respondents detect cyber attacks. Computer Security Institute. [Online]. Available: http://www.gocsi.com/prelen_000321.htm [11.10.2001] Reuvid، Jonathan. (1998). The Regulation and Prevention of Economic Crime، London: Kogan، 14.

لمـدد تـتراوح مـن عـام إلى تسـعة أعـوام أن لا تنتبـه الجهـة التـى قامـت بالتسـجيل إلى انتهـاء فـترة تسـجيل النطـاق ووجـوب التجديـد حيـث توجـد شركات يطلـق عليهـا صائـدو النطاقـات[1] (Domain Hunters) تقـوم بتجديـد النطـاق لهـا ومسـاومة الشركـة الأصليـة فى التنـازل عليـه نظـير آلاف الـدولارات مسـتغلة اعتـماد الشركـة عـلى هـذا الاسـم و معرفـة العمـلاء بـه لمـدد طويلـة هـذا فضـلا عـن الحمـلات الدعائيـة لـه وكـم المطبوعـات الورقيـة التـى أصدرتهـا الشركـة و تحمـل ذلـك العنـوان.[2]

مـن الجرائـم الأخـرى المتعلقـة بأسـماء النطاقـات عـلى شـبكة الانترنـت مـا يعـرف بإعـادة التوجيـه (Redirection) مثلـما حـدث لموقـع شركـة Nike فى شـهر يونيـو عـام 2000 حيـث قامـت جماعـة مـن المحترفـين بالدخـول عـلى موقـع شركـة تسـجيل النطاقـات الشـهيرة و المعروفـة باسـم (Network Solutions) و تغيـير بيانـات النطـاق لضعـف إجـراءات امـن المعلومـات بالشركـة فى ذلـك الحـين و بذلـك تـم إعـادة توجيـه مسـتخدمي الانترنـت إلى موقـع لشركـة انترنـت فى اسـكوتلاندا[3].

---

(1) Philippe JOUGLEDX، droit des médias، faculté de droit d'aix- Marseille، dans le thème :"la criminalité dans le cuber- espace »، 1999، p : 25 et suivants.

(2) برنامج (Net bus): أشهر البرامج وأكثرها انتشارا وقد يكون سبب انتشاره أنه من أوائل البرامج التي ظهرت لهذا الغرض، ولسهولة استخدامه لقي رواجا كبيرا وعلى الرغم من أنه لم يكمل العامين من عمره إلا أنه يوجد العديد من الإصدارات التي تتحسن وتزداد خطـورة في كل إصدارة عن سابقـتها. (Nanoart،2000)

(3) Skinner، W. F.، & Fream، A. M. (1997، November). A social learning theory analysis of computer crime among college students. Journal of research in Crime and Delinquency، 34 (4)، 495 -519 . Staff.(2000،April2).TheBusinessof Technology. Available: http: // www.redherring.com/mag/ issue7/ news - security. html [11.10.2001]. Thomas، P. (2000، February 23). Insufficient computer security threatens doing business

أيضا قامت إحدى الجماعات بعمل موقع على شبكة الانترنت تحت عنوان (http://www.gatt.org) مستخدمة شكل و تصميم الموقع الخاص بمنظمة التجارة العالمية (World Trade Organization) و الذي يظهر كخامس نتيجة فى اغلب محركات البحث عن ال WTO و قد استخدمته للحصول على بيانات البريد الالكتروني وباقي بيانات مستخدمي الانترنت الذين كانوا فى الأصل يبغون زيارة موقع منظمة التجارة العالمية ومازالت القضية معلقة حتى الآن مع المنظمة الدولية لحماية حقوق الملكية الفكرية (World Intellectual Property Organization).

مشكلة البحث:

حين يسعى المرء إلى جمع أدلة تتصل بجريمة ارتكبت مؤخراً، وتصبح المهمة بالغة الصعوبة حين تتجاوز الواقعة او الإختراق ...إلخ، النطاق المكاني للولاية القضائية، كما تدعو الحاجة إلي وسائل متعددة ذات نظم مختلفة في حفظ الأدلة، وهكذا لم تعد تكفي الوسائل التقليدية لإنفاذ القانون، كما أن بيئة التواصل الإجتماعي تسهم بشكل غير مباشر - مقدمي الخدمات الإلكترونية علي الشبكة المعلوماتية - في إستخدامها في بعض الجرائم المعلوماتية[1].

إن بطء الإجراءات وعدم تحديدها، وكذا إيلاء جهة معينة السلطة أو مكنة الإدارة الرسمية لحفظ الأدلة الجنائية يجازف بفقدان الأدلة، وقد تكون بلدان متعددة متورطة في الأمر، ولذا تشكل متابعة وحفظ سلسلة الأدلة تحدياً كبيراً، بل حتى الجرائم"المحلية"قد يكون لها بعد دولي، وربما تكون هناك حاجة إلى طلب المساعدة من جميع البلدان التي مرت الهجمة من خلالها[2].

وإذا كانت هناك جريمة واضحة تستحق التحقيق بالفعل، فقد تكون

---

(1) العلمي عبد الواحد"المبادئ العامة لقانون الجنائي الغربي"طبعة 1998 مطبعة النجاح الجديدة ص 276

(2) محمد بوشيبة، مقالة بعنوان"حماية برامج الحاسوب طبقا لقانون 2.00 المنظم لحقوق المؤلف و الحقوق المجاورة"منشورة بمجلة القضاء و القانون العدد150 سنة 2004.

هناك حاجة إلى مساعدة من السلطات في البلد الذي كان منشأ الجريمة، أو من السلطات في البلد أو البلدان التي عبر من خلالها النشاط المجرَّم وهو في طريقه إلى الهدف، أو حيث قد توجد أدلة الجريمة.

وهناك عنصران أساسيان للتعاون:

- المساعدة غير الرسمية من محقق لآخر.
- والمساعدة الرسمية المتبادلة.

ولاشك أن أول الحلقات التي ينبغي غلقها، والمتمثلة في نوادي الكومبيوتر، ومن خلال المنتديات، وعبر شبكات التواصل[1].

وقد تكون المساعدة غير الرسمية أسرع إنجازاً، وهي الوسيلة المفضلة للنهج حين لا تكون هناك حاجة إلى صلاحيات إلزامية (أي أوامر تفتيش أو طلب تسليم المجرم).

وهي تقوم على وجود علاقات عمل جيدة بين أجهزة شرطة البلدان المعنية، وتولد نتيجة الاتصالات التي جرت مع الوقت في مسار المؤتمرات وزيارات المجاملة والتحقيقات المشتركة السابقة.

ومن ناحية أخرى فإن المساعدة الرسمية المتبادلة هي عملية أكثر إرهاقاً يتم اللجوء إليها عادة عملاً بترتيبات معاهدات بين البلدان المعنية وتشمل تبادل الوثائق الرسمية، وهي تشترط في الغالب الأعم أن تكون الجريمة المعنية على درجة معينة من القسوة وأن تشكل جريمة في كل من البلدان الطالبة والموجه إليها الطلب. ويشار إلى هذا الأمر الأخير باعتباره" تجريماً مزدوجاً".[2]

---

(1) د. محمد أمين الرومي"جرائم الكمبيوتر والانترنت"طبعة 2003 دار المطبوعات الجامعية ص 102.

(2) د. حسين بن سعيد الغافري - جرائم الحاسب الآلي – ورقة عمل مقدمة من الأمانة العامة لمجلس التعاون الخليجي لاجتماع اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم الإلكترونية"الإنترنت"الأول والذي أنعقد بمقر الأمانة العامة بالرياض خلال الفترة من 4-2004/4/5م.

منهج البحث:

إعتمد البحث علي المنهج الإستقرائي التحليلي، حيث أن جرائم المعلوماتية تتميز بالتطور الدائب والدائم، وبالرغم من الإهتمام المتزايد بها إلا أن التطور وإن كان محط إهتمام الباحثين، إلا أنه تطبيقاته العملية محدودة، وبخاصة في مجال العمل الشرطي والقضائي، ولاشك أن تحليل الأطر القانونية أو إيجاد عوامل أخي مساعدة قد يكون له أبلغ الأثر في الحد من تلك الجرائم[1].

(1) Thomas، P. (2000، February 23). Insufficient computer security threatens doing business. Available: http: // www. cnn. com/ 2000/TECK/ computing/ 0223// credir.card.thefts/ index. html [11.11.2001]. Thompson، R. (1999، February). Chasing after petty computer crime. IEEE Potentials، 18 (1)، 2022-.

الفصل الأول

الحماية الجنائية للخصوصية المعلوماتية

تناولنا الحماية الجنائية للمعلومات والمتمثلة فى الجرائم التى قد تقع على النظام المعلوماتى، إلا أنه قد يقتصر النشاط الإجرامى على مجرد إنتهاك الخصوصية والتى تتمثل فى الإطلاع على المعلومات الخاصة بالشخص إما من باب الخطأ أو بقصد التجسس...إلخ، لذا سنعرض لهذه الأفعال فيما يلى:

المبحث الأول: ماهية الخصوصية المعلوماتية وتطورها.

المبحث الثانى: الحماية الجنائية للخصوصية المعلوماتية.

المبحث الثالث: الاعتداء على سرية الخطابات والمراسلات الخاصة.

المبحث الرابع: مواجهة الاعتداءات.

المبحث الأول

ماهية الخصوصية المعلوماتية وتطورها

تعـرف الحـق فى الخصوصيـة [1] المعلوماتيـة فى النظـام اللاتينـى بالحـق فى الحيـاة الخاصـة، ويعـرف بحـق إحـترام سريـة وخصوصيـة الأشـخاص مـن أى تدخـل مـادى أو معنـوى، وهـو حـق أصيـل.

ولقـد جـاءت نشـأة مفهـوم الخصوصيـة، حيـث جـاءت إنجليزيـة الجـذور، فتطـور مفهومهـا فى بريطانيـا وبقـى حبيـس المفهـوم المـادى للخصوصيـة، فى حـين أن الخصوصيـة المعلوماتيـة أمريكيـة التطـور فى النطـاق الفقهـى والدسـتورى، وهـى فرنسـية الإعـتراف كحـق عـام، أمـا بالنسـبة للأنظمـة التشريعيـة فـإن أول مدونـة دسـتورية لحقـوق الإنسـان تتمثـل بوثيقـة الحقـوق البريطانيـة الصـادرة عـام 1215 والمعروفـة بالعهـد الأعظـم (الماجنـا كارتـا)[2].

وفى بريطانيـا عـام 1361 صـدر قانـون The Justices of peace act وبموجبـه تـم منـع إختـلاس النظـر و إسـتراق السـمع وعاقـب عليهـا بالحبـس، وفى السـياق نفسـه وتكريسـا لعـدد مـن مظاهـر الحريـة أقـر فى عـام 1629 نظـام Habes- carpus الـذى قـرر بعـض الحقـوق فى التعامـل مـع السـجناء.

وفى عـام 1719 تـم إدخـال التعديـلات العـشرة عـلى الدسـتور الأمريـكى

(1) وقد ورد حماية الخصوصية فى الشرائع السماوية وكان آخرها ما ورد فى الأية 27 من سورة النور، والأية 12 من سورة الحجرات.د. محمد عبد المحسن المقاطع – حماية الحياة الخاصة للأفراد وضماناتها فى مواجهة الحاسب الآلى- جامعة الكويت – 1992 صـ19 (S.(www.privacy international.org) وبموجبها نزل الملك عن سلطانه المطلقة فمنح عهدا بعدم القبض على أحد أو حبس أو مصادرة أمواله إلا بحكم صادر عن سلطة قانونية.

(2) د. محمد بن مفلح المقدس – الآداب الشرعية والمنح المرعية – دار العلم للجميع – بيروت 1972 صـ19

فيـما عـرف بوثيقـة الحقـوق ومـن بينهـا الحـق فى الخصوصيـة، ويمكـن تقسـيم الخصوصيـة إلى عـدد مـن المفاهيـم المنفصلـة.

خصوصيـة المعلومات Information Privacy:

والتـى تتضمـن القواعـد التـى تحكـم جمـع وإدارة البيانـات الخاصـة كمعلومـات بطاقـات هويـة والمعلومـات الماليـة والسـجلات الطبيـة والسـجلات الحكومية.

الخصوصية الحدسـية أو المادية Bodily Privacy:

والتــى تتعلــق بالحمايــة الجســدية للأفــرار ضــد إجــراءات ماســة بالنواحــى الماديــة لأجســامهم وهــم كفحــص الجينــات Genetic tests وفحــص المخــدرات.

خصوصية الإتصالات Telecommunication privacy:

والتـى تعطى سريـة وخصوصية للمراسـلات الهاتفية والبريد.

ونــرى أن يتــم تضمــين قانــون موحــد للمعلوماتيــة وأن يتضمــن تشــديدا للعقوبـات عـلى أى مسـاس بالخصوصيـة، كـما ان الحاجـة تدعـو إلى تعـاون دولى فى هـذا الشـأن.

وسـنوضح ذلك من خلال الآتي:

المطلب الأول: مفهـوم الخصوصية.

المطلـب الثانى: تطـور الحماية الجنائيـة للمعلوماتية.

المطلب الأول

مفهوم الخصوصية

سنعرض لماهية الخصوصية من خلال تعريفها لغويا ثم إصطلاحا وذلك فيما يلى:

الخصوصية لغة:

حالة الخصوص، يقال خصه بالشئ يخصه خصا، وخصوصا وخصوصية بالفتح والضم، والفتح أفصح ويقال إختص فلان بالآخر إنفراد به والخاصة خلاف العامة ومن مرادفات الخصوصية فى اللغة الإنزواء والانعزال والعزله، والتوحيد والتفرد والأنطواء(1).

وبإضافة لفظ"الحق إلى الخصوصية يمكن أن نتصور معنى هذه الاضافة وهى حق الشخص فى أن ينفرد بأمور لنفسه أو خاصته على ألا تتخذ هذه الاشياء صفة العموم (2).

الخصوصية إصطلاحا:

فقد وردت الخصوصية فى النظام القانونى الأنجلو أمريكى بمعنى (privacy) وفى النظام القانونى اللاتينى عموما (vie privée)(3).

ويكاد ينعقد الإجماع على صعوبة التوصل إلى تعريف جامع مانع للحق

---

(1) إبن منظور – لسان العرب – ط ـ1 منشورات مطبعة بولاق – ج 8 ص 290.

(2) د. عبد اللطيف الهيم -إحترام الحياة الخاصة بين الشريعة الإسلامية والقانون – دار عمان.(www.aldaawah.com)د. عزة محمود خليل – المرجع السابق – صـ262، د. عمر فاروق الحسينى– المرجع السابق صـ 48.

(3) Jacque Velu:- le droit au respect de laveprivée،PrefaceR.GassinTravaux de la faculté de droit 1974 No10.p.70.

فى الحياة الخاصة أو الخصوصية أو السرية الشخصية كما يسميها بعضهم، ولهذا نجد تعريفات متعددة ومتباينة تم وضعها للحق فى الحياة الخاصة وسنعرض للتعريف الفقهى والقضائى.

التعريف الفقهى: لم يتفق الفقه على تعريف جامع مانع للخصوصية، فقد إتجه جانب من الفقه بأنه"حق من طبيعة مادية يرتبط بالشخصية الإنسانية التى لها عليه سلطة تقديرية كاملة"[1].

ذهب إتجاه فى الفقه بأنها"الحق فى أن يترك الشخص وحيدا ولهذا فإن الخصوصية وفق هذا المفهوم تعد أهم سمة من سمات الحرية فى المجتمع الديمقراطى.

وذهب إتجاه"حق الفرد فى أن يختار سلوكه الشخصى وتصرفاته فى الحياة عندما يشارك فى الحياة الإجتماعية مع الآخرين"ثم حدد ثلاث مجموعات رئيسية لهذا الحق وهى:

- حرية التعبير عن الأفكار والإهتمامات الشخصية.
- حرية أن يكون لديه أولاد يربيهم وينشئهم.
- حق الفرد فى الكرامة بدنه وتحريره من القسر والقهر.
- حق الأفراد فى تحديد متى وكيف وإلى أى مدى تصل المعلومات عنهم للآخرين، أو فهو"حق الأفراد أو الجماعات أو المؤسسات فى أن يقرروا بأنفسهم زمن وكيفية ومدى نقل المعلومات عن أنفسهم إلى الآخرين، والخصوصية، منظورا إليها من علاقة الفرد

(1) د. عمر محمد أبو بكر يونس – الجرائم الناشئة عن إستخدام الإنترنت – المرجع السابق – صـ594، د. حسام الدين الأهوانى– الحق فى إحترام الحياة الخاصة – دراسة المقارنة – دار النهضة العربية 1978 صـ480، د. ممدوح خليل بحر – حماية الحياة الخاصة فى القانون الجنائى– دار النهضة العربية 1983 صـ656، د. حسنى الجندى– ضمانات حرمة الحياة الخاصة فى الاسلام – دار النهضة العربية 1993 صـ621 .

بالمشاركة الإجتماعية، هى إنسحاب الفرد الطوعى والمؤقت من المجتمع العام عبر وسائل مادية أو نفسية[1].

ونرى أن يتم تقنين حماية أى مساس بالخصوصية سواء على المستوى المعلوماتى، وبخاصة بعد إنتشار تحميل لصور وأفلام دون الحصول من إذن ممن تم تصويره وبثها على شبكات التواصل الإجتماعى.

---

(1) د. صالح جواد كاظم – التكنولوجيا الحديثة والسرية الشخصية – دار الشئون الثقافية العامة – بغداد 1991 صـ136، د. محمد سامى الشوا – الغش المعلوماتى كظاهرة إجرامية مستحدثة – بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائى– القاهرة 25-28، 1993 صـ170، د. أسامة عبد الله قايد – المرجع السابق- صـ13.

المطلب الثانى

تطور الحماية الجنائية للمعلوماتية

يعتبر الحاسب الآلي واحداً من أهم المخترعات العلمية الحديثة، ولا تكاد تجد مجالاً إلا وقد أفاد من الحاسب الآلي سواء في التعليم، أو الطب، أو الصناعة أو التجارة، أو الزراعة، أو المجالات العسكرية والأمنية، بل في معظم الاحتياجات اليومية.

وكما تطور الحاسب الآلي، تطورت الحماية الجنائية للمعلومات التى تكون هى محتوى البرامج التى تعمل فى تشغيل الحاسب الآلى، وسنعرض لمراحل تطور تلك الحماية فيما يلى:

الحماية الجنائية للمعلومات الإسمية:

وهى مجموعة المعلومات التى تتعلق بالشخص ذاته وتنتمى إلى كيانه كانسان مثل الاسم والعنوان، ورقم الهاتف، وحالة الدخل، والوضع الصحى، والعرق والجنس والعمر والاتجاهات الأخلاقية والسياسية[1]، أو هى معلومات تلتصق وملازمة للشخص الطبيعى فتجعله معروفا أو قابلا للتعريف[2].

صور الإعتداء على الخصوصية:

نشر وإعلان مفردات الحياة الخاصة للشخص فى وسائل الإعلام دون موافقته الصريحة فى كل حالة، أو عدم الإلتزام بحدود هذا الرضاء فيما يتعلق بالتعامل فى المعلومات الشخصية وطرق المعالجة الإلكترونية لها، وما يتعلق من معلومات مثل الصداقات والحالة الصحية والعاطفية والأسرية.

---

(1) S.(www.echo.lu)

(2) د. أيمن فكرى - مرجع سابق - صـ630.

تبـادل المعلومـات والبيانـات فيـما بـين مراكـز المعلومـات وعـدم توافـر الأمـان، وتعـد صـورة الإنسـان مـن أهـم الجوانـب الشـخصية الإنسـانية الجديـرة بالحمايـة.

إسـتقر القضـاء عـلى أن لـكل شـخص حقـا مطلقـا، وقـاصر عـلى صورتـه وعـلى إسـتعمالها وأن الإعتـداء عـلى صـورة الشـخص يكـون الإعتـداء عـلى جـزء هـام مـن الخصوصيـة، وهــو الأمـر الـذى يسـتوجب المسـئولية والعقـاب بحسـب النشـاط المخالـف للحـق فى الخصوصيـة [1].

وفى الولايـات المتحـدة الأمريكيـة، تجـرم تشريعـات بعـض الولايـات مجـرد إسـتراق النظـر ويعـرف مرتكـب، هـذا النـص المقـرر فى القسـم 64 مـن القانـون الجنـائى عـلى أن"يعاقـب مشـددا كل شـخص عمـدا ليـلا أثنـاء تجوالـه أو تسـكعه أو تمضيـة الوقـت إلى النظـر خلسـة مـن بـاب نافـذة مسـكن أو مبنـى مؤجـر مسـكون دون أن يكـون لـه شـأن مـع المالـك أو شـاغل المـكان"

وفى فرنسـا عالـج المـشرع الفرنـسى مسـألة الحمايـة الموضوعيـة للحـق فى صـورة فى المـادة 368 ق.ع.ف القديـم ثـم تـم تعديـل ذلـك بالمـادة 226-2 ويشـترط القانـون لتجريـم إلتقـاط الصـورة أن يكـون قـد تـم فى مـكان خارجـى.

الحماية الجنائيـة للإتصال الخاص:

يعـد إسـتخدام وسـائل الإتصـال الخـاص هـى تلـك التـى يتـم نقـل المحادثـات الشـخصية بـين طرفـين وأمـام التطـور السريـع فى العـصر الحديـث فقـد تعـددت وسـائل الإتصـال الخـاص وتطـورت إمكانياتـه ومنهـا مثـلا البريـد الإلكـترونى وغـرف الدردشـة عـبر الانترنـت والتـى يتـم فيهـا الكتابـة والصـوت أو إضافـة الصـور مـن خلالهـا [2].

---

(1) د. محمد حسين منصور – المرجع السابق – صـ366، ويجرم المشرع الفرنسى فى قانون العقوبات الجديد من هذا الفعل فى المادة 8/226 ق.ع.ف.

(2) S.(www.droit-technologie.org)

وقـد جـرم القانـون الأمريـكى عـلى إنتهـاك الإتصـال الخـاص عـبر الإنترنـت بالقسـم 2710 مـن البـاب 18 وهـو قانـون الخصوصيـة.

أمـا فى القضـاء الفرنـسى فقـد أجـاب بالإيجـاب عـلى خضـوع البـث الخـاص وخاصـة البريـد الإلكـترونى للحمايـة التـى يفرضهـا القانـون عـلى الحـق فى الخصوصيـة، فالقانـون الفرنـسى يميـز بـين البـث الخـاص والبـث العـام بمقتـضى المـادة 2-2 مـن القانـون الصـادر 1986/9/3 والـذى ينـص عـلى أن"يعـد إتصـال سـمعى مـرئى كل إجـراء إتصالى أو إشـارة أو إشـارات مكتوبـة أو أصـوات أو رسـائل مـن كافـة الأشـكال التـى لا تكـون فى هيئـة إتصـال خـاص".

كـما أن المـادة -226 15 مـن قانـون العقوبـات الحديـث تنـص عـلى"كل فعـل إرتكـب يـؤدى بقصـد قطـع أو تحويـل أو إسـتخدام أو نـشر عـن الإتصـالات الخاصـة، والمتراسـلة أو المسـتقبلة بوسـيلة الإتصـالات أو بواسـطة إعـداد أجهـزة مهمتهـا إرتـكاب هـذه الأفعـال".

كـما يسـتخدم القضـاء الفرنـسى هـذا النـص فى حالـة العـدوان عـن طريـق الكوكيـز، وفى مجـال رقابـة الأجـير أو المسـتخدم مـن قبـل رب العمـل فـإن المـادة 121-8 مـن قانـون العمـل الفرنـسى تنـص عـلى أنـه"لا يجـوز إلتقـاط أيـة معلومـات شـخصية تخـص أجـير أو مسـتخدم مـن قبـل صاحـب العمـل مـا لم يكـن قـد تـم إبـلاغ الأجـير أو المسـتخدم سـلفا بذلـك"[1].

(1) انظر: دليل مواقع الإنترنت،منصور محمد محروس،دار العصر، الرياض، الطبعة الثانية، 2000م ص1.انظر: مقدمة في الحاسب الآلي وتقنية المعلومات ص201-216، التنظيم القانوني لشبكة الإنترنت ص55، التجارة على الإنترنت – تأليف / سايمون كولن، نقله إلى العربية / يحيى مصلح، بيت الأفكار الدولية بأمريكا 1999مقدم المؤتمر الثاني عشر للحاسب الآلي المعقود في جامعة الملك سعود عام 1411هـ التوصية الآتية: (ضرورة العمل على تطوير خطة وطنية للمعلوماتية للمملكة العربية السعودية، نظراً لأهمية تقنيات المعلومات الأمنية والإستراتيجية والاقتصادية، وحتى لا تتخلف المملكة عن ركب الدول التي تخطط لنفسها للانتقال إلى عصر المعلومات). ص22.

الحمايـة التقنية للخصوصيـة المعلوماتية:

إن تحقيـق الحمايـة الناجحـة يجـب ألا تقتـصر فقـط عـلى البحـث عـلى الحمايـة الجنائيـة فقـط بـل لابـد مـن السـعى لتوفيرهـا فى مجـال التقنيـة المعلوماتيـة.

مخاطـر خصوصية المعلومـات فى العصر الرقمى:

كتـب الفقيـه الفرنـسى Mellor فى عـام 1972"إن الكومبيوتـر بإتسـاعه لجمـع المعلومـات عـلى نحـو لا يمكـن وضـع حـد لهـا، ومـا يتصـف بـه مـن دقـة واسـتمرار، ومـا يخـزن فيـه يقلـب حياتنـا رأسـا عـلى عقـب يخضـع فيهـا الأفـراد لنظـام رقابـة صـارم ويتحـول المجتمـع بذلـك إلى عـالم شـفاف تصبـح فيـه بيوتنـا ومعاملاتنـا الماليـة وحياتنـا العقليـة والجسـمانية عاريـة لأى مشـاهد [1].

مخاطـر الخصوصيـة فى بيئة الإنترنـت والتجارة الالكترونية:

إن مـن أهـم شروط الخصوصيـة عـدم إطـلاع الآخريـن عـلى مـا يقـوم بـه فى بيئـة المعلومـات، فلـو إفترضنـا أنـك تسـير فى أحـد مخـازن الأسـواق بـين مخـازن عديـدة لا تعـرف أيـا منهـا، فتوضـع عـلى ظهـرك إشـارة تبـين كل محـل زرتـه ومـا الـذى قمـت بـه ومـا إشـتريته، إن هـذا الشـئ شـبيه لمـا يمكـن أن يحصـل فى بيئـة الإنترنـت[2].

(1) S.(www.usdoj.gov)

انظر: التخطيط للمجتمع المعلوماتي،الدكتور / محمد محمود مندورة، جامعة الملك سعود - الرياض 1411هـ.ص22 المعلوماتية بعد الإنترنت (طريق المستقبل) - بيل جيتس، ترجمه عبد السلام رضوان، دارعالم المعرفة الكويت،عام 1418هـ.ص11.

(2) د. عبد الله قايد - الحماية الجنائية للحياة الخاصة وبنوك المعلومات - دار النهضة العربية - 1988 - صـ 48. نظام حماية حقوق المؤلف في المملكة العربية السعودية، إعداد: عبيد الله محمد العبيد الله، ضمن دورة حقوق الملكية الفكرية (الأنظمة والتشريعات) المعقودة بتأريخ 12 / 11 / 1422هـ في مركز الملك فيصل للبحوث والدراسات الإسلامية - معهد الفيصل لتنمية الموارد البشرية.

المبحث الثاني

الحماية الجنائية للخصوصية المعلوماتية

تبرز الأهمية في تحديد معنى الخصوصية والحق[1] في الإحتفاظ بمكنون ما للإنسان من أسرار أو معلومات خاصة به، وانطلاقا من السعي نحو ما إذا كان لهذا المعنى مفاهيم مختلفة في بيئة الحاسب الآلي عما هو عليه في بيئته التقليدية، وما يستتبعه من ضرورة إفراد حماية قانونية خاصة بتلك البيئة، أم أن النصوص القانونية التقليدية كفيلة بالتصدي لأشكال التعدي على هذا الحق، كما حفظت الشريعة الإسلامية الحقوق الشخصية للأفراد، وحرمت الاعتداء عليها، وحرمت تتبع عورات الآخرين، والاطلاع على أسرارهم.

وفي الحديث عن أبي هريرة [2]أن رسول الله ﷺ قال: (إياكم والظن[3]، فإن الظن أكذب الحديث، ولا تحسسوا، ولا تجسسوا[4]، ولا تنافسوا، ولا تحاسدوا، ولا تباغضوا، ولا تدابروا، وكونوا عباد الله إخوانا كما أمركم. المسلم أخو المسلم، لا يظلمه، ولا يخذله، ولا يحقره، التقوى ههنا - ويشير

---

(1) انظر: الفقه الإسلامي وأدلته، للدكتور / وهبة الزحيلي، دار الفكر،دمشق - 1417هـ، 8/4 والحق ومدى سلطان الدولة في تقييده، للدكتور / فتحي الدريني، جامعة دمشق - 1386هـ، ص 184 والمدخل الفقهي العام،مصطفى الزرقاء،دار الفكر، 10/3.

(2) عبد الرحمن بن صخر الدوسي، صحابي جليل، كان أكثر الصحابة حفظاً للحديث ورواية له نشأ ضعيفاً يتيماً، قدم المدينة ورسول الله صلى الله عليه وسلم بخيبر، فأسلم سنة 7هـ، ولزم النبي صلى الله عليه وسلم فروى عنه نحو (5274) حديثاً، ولي إمرة المدينة، ولما صارت الخلافة إلى عمر بن الخطاب -رضي الله عنه- استعمله على البحرين، توفي بالمدينة سنة 59هـ.(انظر: صفة الصفوة 285/1، حلية الأولياء 376/1).

(3) المراد بالظن هنا: التهمة التي لا سبب لها كمن يتهم رجلا بالفاحشة من غير أن يظهر عليه ما يقتضيها وليس المراد بالظن هنا ما يتعلق بالاجتهاد الذي يتعلق بالأحكام أصلاً. (فتح الباري 496/10).

(4) التحسس: الاستماع لحديث القوم، والتجسس: البحث عن العورات.(انظر: لسان العرب، مادة السين، فصل الجيم)

إلى صدره - بحسب امرئ من الشر أن يحقر أخاه المسلم، كل المسلم على المسلم حرام: دمه، وعرضه، وماله، إن الله لا ينظر إلى أجسادكم، ولا إلى صوركم ولكن ينظر إلى قلوبكم وأعمالكم) [1]

أولا: الحماية الجنائية للبيانات الشخصية:

لاشك أن الحماية الشخصية للإنسان لا تنفصل عن حماية حقوقه اللصيقة بشخصيته، وهو ما بلورته النصوص الجنائية، فضلا عن ما قررته الشريعة الغراء من سدها للذرائع فى نهيها عن تتبع عورات البشر، فعن معاوية بن أبي سفيان [2]قال: سمعت رسول الله ﷺ يقول: (إنك إن اتبعت عورات المسلمين أفسدتهم، أوكدت أن تفسدهم)[3] فهذا نهي من الشارع الحكيم عن تتبع عورات المسلمين وبيان أن ذلك سبب لإفسادهم.

و تقتصر الحماية الجنائية فى مجال المعلوماتية على بيانات ومعلومات على سبيل الحصر:

- بيانات الأحوال المدنية.
- بيانات التعداد والإحصاء السكانية.
- البيانات الضريبية.
- بيانات حسابات البنوك والمعاملات المتعلقة بها.

---

(1) رواه البخاري في كتاب الأدب،باب ما ينهى عن التحاسد والتدابر، ورواه مسلم في كتاب البر و الصلة والآداب، باب: تحريم الظن والتجسس والتنافس برقم (2563).

(2) معاوية بن (أبي سفيان) صخر بن حرب بن أمية القرشي الأموي، أحد الصحابة الأجلاء، أسلم يوم الفتح، كان من كتاب الوحي، ولاه عمر على الأردن ثم على دمشق، وولاه عثمان على الديار الشامية كلها مات - رضي الله عنه - في دمشق سنة 60هـ، له 130 حديثاً.(انظر: تأريخ ابن الأثير 2/4، وتاريخ الطبري180/6).

(3) رواه أبو داود، حديث رقم (4888)، وقال عنه النووي: إسناده صحيح.(انظر: رياض الصالحين باب النهي عن التجسس، ص596).

- وإقرارات الكسب غير المشروع.

- بيانات المعلومات غير المعلنة أوالخصوصية المعلوماتية.

أولا: بيانات الأحوال المدنية:

تنص المادة التاسعة من القانون رقم 206 لسنة 1960 فى شأن الأحوال المدنية المعدل بالقانون رقم 11 لسنة 1965 والقانون رقم 158 لسنة 1980 على أن....، وتعتبر سرية ما تحتويه هذه السجلات من بيانات.....

وقد جاء بالمذكرة الإيضاحية لهذا القانون رقم 260 لسنة 1960 على أنه"لما كانت هذه السجلات تحوى أدق البيانات عن حالة الشخص [1]، فقد أسبغت عليها السرية حتى يطمئن كل شخص على ما يقدمه من بيانات، ومفهوم أن نطاق السرية يمتد إلى كل ما لا يفرضه عليه واجبه - طبقا لقانون الأحوال المدنى ولائحته التنفيذية والقرارات المنفذة له - الإطلاع على هذه البيانات، وذلك ما لم تصدر السلطة القضائية أو سلطة التحقيق قرارا بالإطلاع عليها أو فحصها لأن الصالح العام يقدم على المصلحة الشخصية فى المحافظة على سرية تلك المعلومات، وبإعتبار تلك البيانات سرا فإن إفشائها من قبل الموظف المختص بالمحافظة على سريتها، يوقعه تحت طائلة العقاب بالمادة 310 ق.ع.م[2].

كما تدخل المشرع مرة أخرى بالقانون رقم 143 لسنة 1994 لحماية البيانات والمعلومات الخاصة بمصلحة الأحوال المدنية وذلك من الإعتداء على حاسبتها وشبكاتها التى تضم تلك المعلومات فنص فى المادة 13 من هذا القانون على أن"تعتبر البيانات والمعلومات المتعلقة بالأحوال المدنية للمواطنين والتى تشمل عليها السجلات أو الدفاتر أو الحاسبات الآلية أو

---

(1) Jerry Berman، Deidre Mulligan: Privacy in the digital age، Work in progress، Nova law review، Vol.23، 1999،p4.

(2) الخصوصية في عصر المعلومات، فريده كيت - ترجمة / محمد محود شهاب، مركز الأهرام لترجمة والنشر الطبعة الأولى، ص14، د. هشام فريد رستم - المرجع السابق - صـ370.

وسـائط التخزيـن الملحقـة سريـة ولا يجـوز الإطـلاع أو الحصـول عـلى بيانهـا إلا فى الأحـوال التـى نـص عليهـا القانـون وفقـا لأحكامـه[1].

وإذا أصـدرت إحـدى جهـات القضـاء أو النيابـة العامـة قـرار بالاطـلاع عـلى السـجلات المشـار إليهـا أو بفحصهـا يجـب أن ينتقـل القـاض المنتـدب أو المحقـق للإطـلاع أو الفحـص فى الجهـة المحفـوظ بهـا السـجلات أو أن يطلـب صـورة قيـد الواقعـة أو البيانـات المسـجلة أو صـورة طبـق الأصـل مـن المسـتند الـذى أدخلـت بيانـه بالسـجلات إلا إذا كان هـذا المسـتند محـلا للتحقيـق فى تزويـر[2].

وقـد نـص المـشرع بالمـادة 74 عـلى تجريـم تلـك الأفعـال التـى تقـع عـلى المعلومـات وبيانـات خاصـة بمصلحـة الأحـوال المدنيـة فنـص عـلى أنه"مـع عـدم الإخـلال بأيـة عقوبـة أشـد منصـوص عليهـا فى قانـون العقوبـات أو غـيره مـن القوانـين يعاقـب بالحبـس مـدة لا تتجـاوز سـتة أشـهر وبغرامـة لا تزيـد عـن خمسـمائة جنيـه أو بإحـدى هاتـين العقوبتـين، كل مـن إطلـع أو شرع فى الإطـلاع أو حصـل أو شرع فى الحصـول عـلى بيانـات أو المعلومـات التـى تحتويهـا.......

ونـص المـادة 75 مـن القانـون عـلى أن"يعاقـب... كل مـن يحصـل أو أتلـف الشـبكة الناقلـة لمعلومـات الأحـوال المدنيـة أو جـزء منهـا، وكان ذلـك ناشـئا عـن إهمالـه أو رعونتـه أو عـدم مراعاتـه للقوانـين واللوائـح والأنظمة"ويشـدد العقـاب فى حالـة مـا إذا وقـع الفعـل بطريقـة العمـد[3].

ونلخـص مـما سـبق أن: المـشرع المـصرى فى هـذا القانـون قـصره عـلى البيانـات

---

(1) كذلك من الوسائل الفاعلة في حماية الخصوصية الاحتجاج العام، ففي عام 1991م، تخلت شركة لوتس للتنمية و شركة إكويفاكس عن خططهما لبيع قاعدة بيانات على قرص مدمج باسم (المنازل الأسرية) تحتوي على أسماء، وعناوين، ومعلومات تسويقية عن 120 مليون مستهلك، وذلك بعد تلقي 30000 مكالمة هاتفية وخطاب من أفراد يطلبون استبعادهم من قاعدة البيانات.

(2) حق الابتكار في الفقه الإسلامي المقارن، للدكتور / فتحي الدريني، مؤسسة الرسالة، الطبعة الثالثة عام 1404هـ، ص 9. د. أيمن عبد الحفيظ - المرجع السابق - صـ215.

(3) د. عزه محمود خليل - مرجع سابق - صـ273.

الشخصية التى تقضى إجراء إحصاء أو تعداد سكانى، والبيانات والمتعلقة بالأحوال المدنية للمواطنين، ولا يجوز القياس عليها أو التوسع فى تفسيرها وفقا للمبادئ القانونية المستقرة فى القانون الجنائى.

ويرى جانب من الفقه أن: حماية الحياة الخاصة منصوص عليها فى المادة 309 مكرر ق.ع.م[1].

ونرى أنه: فى إطار المتغيرات الراهنة، وما تقتضيه من الشفافية والإفصاح، أن يتم تحديد ما يمكن إتاحته بنصوص محددة، وأن يتم تشديد العقوبة على أى إنتهاك للخصوصية، فيما عدا ذلك.

البيانات الضريبية وإقرارات الكسب غير المشروع:

تنص المادة 146 من قانون الضرائب على الدخل رقم 157 لسنة 1981 على أن"كل شخص يكون له بحكم وظيفته أو إختصاصه أو عمله شأن فى ربط أو تحصيل الضرائب المنصوص عليها فى هذا القانون أو الفصل فيما يتعلق بها من منازعات ملزم بمراعاة سر مهنته ولا يجوز لأى من العاملين بمصلحة الضرائب من يتصل عملهم بربط أو تحصيل الضريبة إعطاء أى بيانات أو إطلاع الغير على أى ورقة أو بيان أو سلف أو غيره، إلا فى الأحوال المصرح بها قانونا.

وكذلك تنص المادة 11 من القانون رقم 11 لسنة 1968 بشأن الكسب غير المشروع على أن الإقرارات المنصوص عليها فى هذا القانون وما أجرى فى شأنها من فحص وتحقيق، تعتبر من الأسرار المؤتمن عليها، ويجب على كل من له شأن فى تنفيذ هذا القانون عدم إفشائها، ويقع من يخالف تحت طائلة العقاب بالمادة 310 ق.ع.م بإعتباره أمينا على السر وأفشاه"[2].

---

(1) د. أيمن فكرى – المرجع السابق – صـ743.

(2) د. هشام محمد فريد رستم – قانون العقوبات ومخاطر تقنية المعلومات مكتبة الآلات الحديثة 1992 صـ 180.

بيانات التعداد والإحصاءات السكانية:

نص المشرع على حماية البيانات التى تجمع لأغراض التعداد والإحصاءات السكانية بالسرية بالمادة الثالثة من قرار رئيس الجمهورية بالقانون رقم 35 لسنة 1960 بشأن الإحصاء والتعداد المعدل بالقانون رقم 28 لسنة 1982 على أن"البيانات الفردية التى تتعلق بأى تعداد أو إحصاء سرية لا يجوز إطلاع أى فرد أو هيئة عامة أو خاصة عليها أو إبلاغ شئ منها، و لايجوز إستخدمها لغير الأغراض الإحصائية أو نشر ما يتعلق منها بالأفراد الا بمقتضى إذن كتابى من ذوى الشأن، و لايجوز كذلك إستخدام أى بيان إحصائى كأساس لربط ضريبة أو لترتيب أى عبء مالى آخر ولا إتخاذه دليلا فى جريمة أو أساس لأى عمل قانونى[1].

وتنص المادة الرابعة من القرار المذكور والمعدلة بالقانون رقم 28 لسنة 1982 عقوبة الحبس مدة لا تقل عن شهر ولا تزيد على ستة أشهر وغرامة لا تقل عن مائة جنيه و لا تجاوز خمسمائة جنيه أو احدى هاتين العقوبتين.

كل من أخل بسرية البيانات الإحصائية أو أفشى بيانا من البيانات - الفردية وسر من أسرار الصناعة أو التجارة وغير ذلك من أساليب العمل التى يكون إطلع عليها بمناسبة عمله فى الإحصاء أو التعداد.

كل من حصل بطريقة الغش أو التهديد أو الإيهام أو بأية وسيلة أخرى على بيانات أو معلومات سرية بشأن الإحصاءات أو التعدادت أو شرع فى ذلك.

ونرى ضرورة تشديد العقوبة، ورفع قيمة الغرامة المالية، وتحديد أطار قانونى للإهمال فى حفظ هذه المعلومات.

---

(1) د. علاء عبد الباسط خلاف - مرجع سابق - صـ177-182

بيانات حسابات البنوك والمعاملات المتعلقة بها:

تنص المادة الأولى من القانون رقم 205 لسنة 1990 بشأن سرية الحسابات البنكية على أن"تكون جميع حسابات العملاء وودائعهم وأماناتهم وخزائنهم فى البنوك وكذلك المعاملات المتعلقة بها سرية و لا يجوز الإطلاع عليها أو إعطاء بيانات عنها بطريق مباشر إلا بإذن من صاحب الحساب أو الوديعة أو الأمانة أو الخزينة أو من أحد ورثته أو من أحد الموصى لهم بكل أو بعض هذه الأموال أو من النائب القانونى أو الوكيل المفوض فى ذلك بناء على حكم قضائى أو حكم محكمين.

تنص المادة الثانية من هذا القانون على أن"البنوك تفتح حسابات حرة مرقمة بالنقد الأجنبى أو ربط ودائع منها وقبول ودائع مرقمة بالنقد المذكور وتحظر أن يعرف أسماء أصحاب هذه الحسابات والودائع غير المسئولين بالبنك الذى يصدر بتحديدهم قرار من مجلس إدارته.

ولا يجوز فى جميع الأحوال الكشف عن شخصية صاحب الحساب أو الوديعة المرقمة إلا بإذن كتابى منه أو من أحد ورثته أو من أحد الموصى لهم بكل أو بعض هذه الأموال أو من النائب القانونى أو الوكيل أو المفوض فى ذلك بناء على حكم قضائى أو حكم محكمين نهائى ويسرى الحظر المنصوص عليه فى الفقرة الأخيرة من المادة الأولى على هذه الحسابات والودائع.

كما تعهد المادة الرابعة لمجلس إدارة البنك المركزى المصرى وضع القواعد المنظمة لتبادل البنوك للمعلومات معه، وفيما بينها للمعلومات والبيانات المتعلقة بمديونية عملائها والتسهيلات الإئتمانية المقررة لهم بما يكفل سريتها ويضمن توافر البيانات اللازمة لسلامة منح الإئتمان المصرفى[1].

---

(1) انظر: الحماية الجنائية للتجارة الإلكترونية للدكتور / مدحت عبد الحليم رمضان، ص131، دار النهضة العربية – القاهرة. الصحوة الإسلامية – ضوابط وتوجيهات – للشيخ محمد بن صالح بن عثيمين ص178، دار القاسم – الطبعة الثالثة – 1416هـ.

تنص المادة الخامسة على: رؤساء و أعضاء مجالس إدارة البنوك ومديروها والعاملين بها فى غير الحالات المرخص لها بمقتضى أحكام هذا القانون ويسرى هذا الخط على كل من يضطلع بحكم مهنته أو وظيفته أو عمله بطريق مباشر أو غير مباشر على البيانات والمعلومات المشار إليها.

تنص المادة السابعة على أنه:"مع عدم الإخلال بأى عقوبة أشد يعاقب كل من يخالف أحكام المادة الأولى والثانية فقرة أخيرة والمادة الخامسة من هذا القانون بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن عشرة آلاف جنيه ولا تزيد على عشرين ألف جنيه.

على أن استخدام الحاسب الآلي في الشر والإضرار بالآخرين وبث الفساد سواء الفساد العقدي أو الفكري أو الأخلاقي لا يجوز، وهو محرم شرعاً.

المبحث الثالث

الاعتداء على سرية الخطابات والمراسلات الخاصة

من أخطر الجرائم التي يمكن أن تقع عن طريق الإنترنت جريمة الاعتداء على الحياة الخاصة، نظراً لعدم وجود الحماية التقنية الفاعلة لما يتم تداوله من معلومات وأسرار ومراسلات بطريق الإنترنت، وتشمل جريمة الاعتداء على الحياة الخاصة الاعتداء بالتنصت أو التسجيل، أونقل لحديث صدر عن شخص أو مراسلة دون رضاه بواسطة جهاز معين، أو التقاط أو نقل صورة شخص تواجد في مكان معين دون رضاه[1].

ولعل المقصود من الحياة الخاصة ما يقوم به الشخص ولا يرتضي أن يطلع عليه الغير. [2]

ونجد أن بعض الناس يحاول أن يعتدي على أسرار الآخرين ويقوم عن طريق وسائل معينة بالتنصت على محادثات تتم عن طريق الانترنت، ويقوم بتسجيل ذلك ثم نشره على العامة من الناس الذي يتعاملون بالإنترنت[3].

ومن الطرق التي تتم في الإنترنت للتنصت على الآخرين استخدام برنامج معين يقوم بفتح منفذ في جهاز الشخص المعتدى عليه ، يمكن من خلاله الاطلاع والاستماع إلى جميع المحادثات والمراسلات الصادرة من الشخص المعتدى عليه ويتم إدخال هذا الملف إلى جهاز المعتدى عليه عن طريق البريد الالكتروني ، أو عن طريق مواقع مغرية يزورها المعتدى عليه

---

(1) الإنترنت والتجارة الإلكترونية – صلاح حامد رمضان على – نشرة تصدر عن شركة الراجحي المصرفية للاستثمار ص34، العدد: 12 / ذو الحجة / 1421هـ

(2) انظر: جرائم الاعتداء على الأشخاص والإنترنت، دكتور / مدحت رمضان، دار النهضة العربية القاهرة، 2000م، ص101-125.

(3) انظر: جرائم الكمبيوتر والإنترنت، محمد أمين الرومي، دار المطبوعات الجامعية، الإسكندرية، عام 2003م، ص140.

فيقـوم بتنزيـل بعـض البرامـج ومنهـا برنامـج التنصـت أو عـن طريـق برامـج المحادثـة فيقـوم المعتـدي بإغـراء المعتـدى عليـه بـأن هـذه البرامـج تحتـوي عـلى ألعـاب مثـيرة أو غـير ذلـك فينخـدع المعتـدى عليـه ويقـوم باسـتقبال الملـف [1]، وسـنعرض لنتائـج الإعتـداء عـلى سريـة الخطابـات والمراسـلات وعـلى رأسـها التشـهير بالأشـخاص، أو الحمايـة للمعلومـات غـير المعلنـة.

ونـرى أن يتـم التعـاون دوليـا لوضـع بروتوكـولات لضـمان حفـظ المعلومـات، وأن يتـم عقـد إتفاقيـات دوليـة للتسـليم فى جرائـم إنتهـاك الخصوصيـة، وأن لا تخضـع مثـل هـذه الجرائـم للتقـادم سـواء للدعـوى أو للعقوبـة.

وسـنعرض لذلك من خلال التالي:

المطلب الأول: التشـهير بالأشخاص.

المطلـب الثاني: حماية المعلومـات غير المعلنة.

---

(1) انظر: مجلة (أون لاين) العدد الرابع عشر، أكتوبر 2001م، ص36،37.

المطلب الأول

التشهير بالأشخاص

التشهير في اللغة: مأخوذ من شهره، بمعنى: أعلنه وأذاعه، وشهّر به: أذاع عنه السوء. [1]

والأصل أن تشهير الناس بعضهم ببعض بذكر عيوبهم ومثالبهم والتنقص منهم حرام، فإذا كان المشهر به بريئاً مما يشاع عنه ويقال فيه، فإن التشهير به محرم لقول الله تعالى: ﴿إِنَّ الَّذِينَ يُحِبُّونَ أَنْ تَشِيعَ الْفَاحِشَةُ فِي الَّذِينَ آمَنُوا لَهُمْ عَذَابٌ أَلِيمٌ فِي الدُّنْيَا وَالْآخِرَةِ وَاللَّهُ يَعْلَمُ وَأَنْتُمْ لَا تَعْلَمُونَ﴾[2]، ولقد قال النبي ﷺ: (أيما رجل أشاع على رجل مسلم كلمة وهو منها بريء، يرى أن يشينه بها في الدنيا، كان حقاً على الله تعالى أن يرميه بها في النار) [3].

وقد ذم الله عز وجل الذين يفعلون ذلك، وتوعدهم بالعذاب الأليم قال ابن كثير[4] في قول الله تعالى: ﴿وَالَّذِينَ يُؤْذُونَ الْمُؤْمِنِينَ وَالْمُؤْمِنَاتِ بِغَيْرِ مَا اكْتَسَبُوا فَقَدِ احْتَمَلُوا بُهْتَانًا وَإِثْمًا مُبِينًا﴾[5]: أي ينسبون إليهم ما هم برآء منه لم يعملوه ولم يفعلوه، يحكون عن المؤمنين والمؤمنات ذلك على سبيل العيب والتنقص منهم، حَدَّثَنَا أَحْمَدُ بْنُ سَلَمَةَ، حَدَّثَنَا أَبُو كُرَيْبٍ، حَدَّثَنَا مُعَاوِيَةُ بْنُ

---

(1) انظر: لسان العرب، والمصباح المنير، والمعجم الوسيط، مادة: (شهر).

(2) سورة النور، الآية: 19.

(3) أخرجه الطبراني وإسناده جيد كما في الترغيب والترهيب للمنذري 157/5.

(4) ابن كثير هو: إسماعيل بن عمر بن كثير بن ضوّ بن درع القرشي البصري ثم الدمشقي، أبو الفداء عماد الدين، حافظ مؤرخ فقيه، ولد في قرية من أعمال بصرى الشام سنة 701هـ، وانتقل مع أخ له إلى دمشق سنة 607هـ، ورحل في طلب العلم، من كتبه: البداية والنهاية، وشرح صحيح البخاري -لم يكمله- وطبقات الفقهاء الشافعيين، وتفسير القرآن الكريم، واختصار علوم الحديث، وغيرها، توفي بدمشق سنة 774هـ. (انظر: شذرات الذهب 231/6، الأعلام 320/1).

(5) سورة الأحزاب، الآية: 58.

هشَام، عَنْ عُمْرَانَ بْنِ أَنَس، عَنِ ابْنِ أَبِي مُلَيْكَةَ، عَنْ عَائِشَةَ، قَالَتْ: قَالَ رَسُولُ اللَّهِ ﷺ لأَصْحَابِه:"أَيُّ الرِّبَا أَرْبَى عِنْدَ اللَّهِ ؟"، قَالُوا: اللَّهُ وَرَسُولُهُ أَعْلَمُ، قَالَ:"أَرْبَى الرِّبَا عِنْدَ اللَّهِ اسْتِحْلَالُ عِرْضِ امْرِئٍ مُسْلِم [1]، ثُمَّ قَرَأَ: وَالَّذِينَ يُؤْذُونَ الْمُؤْمِنِينَ وَالْمُؤْمِنَاتِ بِغَيْرِ مَا اكْتَسَبُوا فَقَدِ احْتَمَلُوا بُهْتَانًا وَإِثْمًا مُبِينًا"[2]، وقد قيل في معنى قول النبي ﷺ: (من سمّع، سمّع الله به) [3] أي من سمّع بعيوب الناس وأذاعها أظهر الله عيوبه. [4]

حتى وإن كان المشهر به يتصف بما يقال عنه ولكنه لا يجاهر به، ولا يقع به ضرر على غيره، فالتشهير به حرام لأنه من الغيبة التي نهى الله سبحانه وتعالى عنها في قوله: ﴿يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيراً مِنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَجَسَّسُوا وَلَا يَغْتَبْ بَعْضُكُمْ بَعْضاً أَيُحِبُّ أَحَدُكُمْ أَنْ يَأْكُلَ لَحْمَ أَخِيهِ مَيْتاً فَكَرِهْتُمُوهُ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَحِيمٌ﴾[5]، ومن المقرر شرعاً أن الستر على المسلم واجب لمن ليس معروفا بالأذى والفساد، فقد قال النبي ﷺ: (من ستر مسلماً ستره الله عز وجل يوم القيامة). [6]

أما إن كان التشهير على سبيل النصيحة للمسلمين وتحذيرهم، كجرح الرواة والتحذير من أرباب البدع والتصانيف المضلة لئلا يغتر بهم، فليس الستر هنا بمرغوب فيه ولا مباح[7]، فأرباب البدع والتصانيف المضلة ينبغي أن يشتهر في الناس فسادها وعيبها، وأنهم على غير الصواب، ليحذرها الناس فلا يقعوا فيها، بشرط أن لا يتعدى فيها الصدق، ولا يفترى على أهلها من

---

(1) حديث (أربى الربا..) أخرجه أبو يعلى بهذا اللفظ، ورواته رواة الصحيح كما قال المنذري في الترغيب والترهيب 504/3، ورواه أبو داود 193/5، والإمام أحمد في المسند 190/1، وحسن إسناده السيوطي (انظر: فيض القدير 531/2).

(2) سورة الأحزاب آية 58

(3) أخرجه البخاري 128/13 من الفتح، والإمام مسلم 2289/4.

(4) مختصر تفسير ابن كثير 114/3.

(5) سورة الحجرات، الآية: 12.

(6) أخرجه البخاري 197/5، وأخرجه الإمام مسلم 1996/4.

(7) انظر: الحطاب 164/6، والآداب الشرعية 226/1.

الفسـوق والفواحـش مـا لم يفعلـوه، بـل يقتـصر عـلى مـا فيهـم مـن المنفـرات خاصـة، ويجـوز وضـع الكتـب في جـرح المجروحـين مـن رواة الحديـث والأخبـار لطلبـة العلـم ولمـن ينتفـع بـه، بـشرط أن تكـون النيـة خالصـة للـه تعـالى في نصيحـة المسـلمين في ضبـط الشريعـة أمـا إذا كان لأجـل عـداوة أو تفكـه بالأعـراض وجريـاً مـع الهـوى، فذلـك حـرام وإن حصلـت بـه المصلحـة عنـد الـرواة [1]

---

(1) انظر: الفروق للقرافي 206/4. انظر: الإنترنت والقانون الدولي الخاص: فراق أم تلاق ؟، للدكتور / أحمد عبد الكريم سلامة، ضمن أبحاث مؤتمر (القانون والكمبيوتر والإنترنت) المجلد الثاني، ص28.التجارة الإلكترونية، تأليف / روب سميس، و مارك سبيكر، ومارك تومسون - ترجمة: د/ خالد العامري، دار الفاروق للنشر والتوزيع، القاهرة - مصر، عام 2000م، ص 98.

المطلب الثاني

حماية المعلومات غير المعلنة

إن هـذه الشـبكة مـع حداثتهـا فـإن عـدد المسـتخدمين قـد بلـغ مطلـع 2002م أكـثر مـن 2133 مليـون مسـتخدم عـلى مسـتوى العـالم.

ولا يعنـى الإسـتخدام مجـرد الولـوج إلى المعلومـات المتاحـة فقـط، بـل إخـتراق المواقـع غـير المتاحـة أو التعـدى إلى البرامـج المحميـة طبقـا للأنظمـة الخاصـة بحمايـة الملكيـة الفكريـة، فقـد نصـت المـادة 61 مـن القانـون 82 لسـنة 2002 والخـاص بإصـدار قانـون حمايـة الملكيـة الفكريـة عـلى أنـه".... يعاقـب كل مـن يقـوم بوسـيلة غـير مشروعـة بالكشـف عـن المعلومـات المحميـة طبقـا لأحـكام هـذا القانـون أو بحيازتهـا أو بإسـتخدمها مـع علمـه بسريتهـا و بأنهـا متحصلـة مـن تلـك الوسـيلة [1].

محل الجريمة:

يحمـى القانـون الخـاص بحمايـة الملكيـة الفكريـة المعلومـات غـير المفصـح عنهـا ويشـترط فيهـا الـشروط الآتيـة:

- أن تتصـف بالسريـة بـأن تكـون المعلومـات فى مجموعهـا أو تكوينهـا الـذى يضـم مفرداتهـا ليسـت معروفـة أو غـير متداولـة بشـكل عـام.
- أن تسـتمد قيمتهـا التجاريـة من كونها سرية.
- أن تعتمـد فى سريتهـا عـلى مـا يتخـذه حائزهـا القانـونى مـن إجـراءات للحفـاظ عليهـا[2].

---

(1) د. محمد حسين منصور – المرجع السابق – صـ376. التعاقد عن طريق وسائل الاتصال الفوري وحجيتها في الإثبات المدني، دراسة مقارنة، للدكتور / عباس العبودي، مكتبة دار الثقافة والنشر والتوزيع، عمان، الأردن ص40.

(2) منشور الجريدة الرسمية العدد 22 مكرر فى 2002/6/2.

1. الركن المادى:

يتمثل الركن المادى فى تلك الجريمة بقيام الجانى بالحصول على المعلومات من أماكن حفظها بأية طريقة من الطرق غير المشروعة كالسرقة أو التجسس، أو إستخدام الغير لتلك المعلومات مع علمه بسريتها وأنها متحصلة بطريق من الطرق غير المشروعة السابقة ويترتب على ذلك كشف للمعلومات أو حيازتها، أو إستخدامها بمعرفة الغير الذى لم يرخص له بذلك [1].

2. الركن المعنوى:

يلزم لهذه الجريمة توافر القصد الجنائى من علم وإرادة متجهة لإرتكاب الفعل الإجرامى بحسب ما ورد فى النص القانونى.

نلخص مما سبق أن: القانون يحمى جانب من جوانب الخصوصية فى مجال المعلوماتية هو تلك المعلومات التى تتسم بالسرية فى المجال الصناعى والتجارى، ولذلك فقد حاول المشرع المصرى أن يتناول جانب آخر يتعلق بحماية الخصوصية المعلوماتية وذلك فيما يتعلق بالبيانات المعالجة إلكترونيا فى نطاق التجارة الإلكترونية بالمحافظة على سريتها وخصوصيتها[2].

---

(1) محمد حسين منصور – مرجع سابق – صـ374.

(2) د. هدى قشقوش – الحماية الجنائية للتجارة عبر الانترنت – دار النهضة العربية 2000 صـ36.دور البنية التحتية للمفاتيح العمومية في دعم الحكومة الإلكترونية في المملكة – د/ محمد بن إبراهيم السويل، ضمن البحوث المقدمة للقاء الحكومة الإلكترونية المعقود بمعهد الإدارة العامة بالرياض، يوم الثلاثاء 1422/11/15هـ. المخاطر الأمنية وطرق الحماية منها – تركي بن أحمد العصيمي – دار المعارج – الرياض – الطبعة الأولى – عام 1420هـ، ص39.

المبحث الرابع

مواجهة الاعتداءات

وبالاطلاع على بعض الإحصائيات لعدد مستخدمي وسائل تقنية المعلومات نعلم أن الاعتماد على هذه الوسائل في أكثر شؤون العمل والحياة سمة غالبة لأكثر الناس اليوم، وذلك بسبب ما تقدمه هذه التقنيات من توفير للجهد والمال والوقت وذلك بالقيام بأعمال كثيرة وبدقة متناهية في وقت قصير، وسنعرض لذلك من خلال إستعراضنا لما يلى سن العقوبات، المراقبة التقنية، تدريب الكوادر[1]، وذلك من خلال الآتي:

المطلب الأول: المواجهة التشريعية.

المطلب الثاني: المراقبة التقنية.

المطلب الثالث: التدريب والتأهيل.

(1) التوقيع الإلكتروني، د/ أحمد شرف الدين، مؤتمر التجارة الإلكترونية والإفلاس عبر الحدود القاهرة، عام 2000م، ص1.

المطلب الأول

المواجهة التشريعية

لا يمكن لأي بلد في هذا العصر أن يعيش معزولاً عن التطورات التقنية المتسارعة، والآثار الاقتصادية، والاجتماعية، والأمنية الناجمة عنها، وفي ظل الترابط الوثيق بين أجزاء العالم عبر تقنيات المعلومات والاتصالات والتطبيقات التي سمحت بانسياب الأموال والسلع والخدمات والأفكار والمعلومات بين مستخدمي تلك التقنيات، بات من الضروري لكل بلد حماية أفراده ومؤسساته ومقدراته وحضارته من آثار هذا الانفتاح، ومع إدراك الجميع اليوم للفوائد الجمة لتقنية المعلومات، فإن المخاطر الكامنة في تغلغل هذه التقنية في بيوتنا ومؤسساتنا تتطلب من المجتمع والدولة جميعاً الحيلولة دون حصول تلك المخاطر بشتى أنواعها ومن أهم ما يجب توفيره في هذا الصدد الأحكام والأنظمة واللوائح المنظمة لسلوك الأفراد والمؤسسات حيال التعامل مع تقنية المعلومات، مهما كان نوع التعامل وأياً كانت مقاصده، دون تقييد لحرية المجتمع عن الاستثمار البناء لتلك التقنية.

لا توجد بصورة منظمة ومعلنة أقسام أمنية ومحاكم مختصة ومنتجات إعلامية لشرائح المجتمع المختلفة [1]، ولقد صدرت في المملكة العربية السعودية بعض الأنظمة واللوائح والتعليمات والقرارات لمواجهة الاعتداءات الإلكترونية، ونصت تلك الأنظمة على عقوبات في حال المخالفة لهذه الأنظمة والتعليمات واللوائح فمن ذلك:

نظام حماية حقوق المؤلف الصادر بموجب المرسوم الملكي رقم (م/11) وتاريخ 1410/5/19هـ، وهذا النظام يمنع جميع صور استنساخ البرامج،

---

(1) دراسة الوضع الراهن في مجال أحكام في المعلوماتية، إعداد: د/ محمد القاسم، د/ رشيد الزهراني عبدالرحمن السند، عاطف العمري، مشروع الخطة الوطنية لتقنية المعلومات، ص6،7.

وإذا تـم ضبـط أي مخالفـة مـن منشـأة تجاريـة، أو مصانـع، أو شركات تعتمـد عـلى الحاسـب الآلي في أعمالهـا وتسـتخدم برامـج غـير أصليـة في تشـغيل الجهـاز، فإنهـا سـتكون عرضـة لتطبيـق العقوبـات الـواردة في النظـام فقـد نصـت المـادة (الثامنـة والعـشرون) مـن النظـام عـلى العقوبـات التـي يمكـن إيجازهـا بمـا يـلي:

- يعاقـب المعتـدي بغرامـة ماليـة لا تتجـاوز عـشرة آلاف ريـال، أو بإغـلاق المؤسسـة أو المطبعـة التـي اشـتركت في الاعتـداء لمـدة لا تتجـاوز خمسـة عـشر يومـاً، أو بالعقوبتـين معـاً، بالإضافـة إلى تعويـض صاحـب الحـق عـما لحقـه مـن ضرر.
- يعاقـب المعتـدي في المـرة الثانيـة بغرامـة ماليـة لا تتجـاوز عشريـن ألـف ريـال، أو بإغـلاق المؤسسـة لمـدة لا تتجـاوز تسـعين يومـاً، أو بهـما معـاً إضافـة إلى التعويـض المـالي لصاحـب الحـق.
- يجـوز أن تأمـر لجنـة النظـر في المخالفـات بمصـادرة، أو إتـلاف جميـع النسـخ غـير الأصليـة، والتـي تـم نسـخها عـن طريـق الاعتـداء عـلى حـق المؤلـف[1].

مـشروع نظـام المبادلات الإلكترونية والتجـارة الإلكترونية[2]:

فقـد نصـت المـادة (20) مـن مـشروع النظـام عـلى أنـه: يعتـبر مرتكبـاً جنايـة أي شـخص يدخـل عـن عمـد منظومـة حاسـوب، أو جـزء منهـا بـدون وجـه حـق، وذلـك بالتعـدي عـلى إجـراءات الأمـن، مـن أجـل ارتـكاب عمـل يعتـبر جنايـة حسـب الأنظمـة المرعيـة وحسـب مـا تحـدده اللائحـة التنفيذيـة.

---

(1) انظر: نظام حماية حقوق المؤلف – مصلحة مطابع الحكومة – المملكة العربية السعودية، 1413هـ. وانظر: نشرة إدارة حقوق المؤلف: هل تعلم أن نسخ أو استخدام البرامج المنسوخة وغير الأصلية لا يجوز شرعاً.

(2) وقد كلف الباحث من قبل وزارة التجارة بالمشاركة في إعداد هذا النظام، فشارك في صياغته، و قد تم رفع المشروع للجهات العليا لإعتماده.

ونصت المادة (21) من مشروع النظام على أنه يعتبر مرتكباً جناية أي شخص يعترض عمداً وبدون وجه حق وعن طريق أساليب فنية، إرسال البيانات الحاسوبية غير المصرح بها للعموم من منظومة حاسوب أو داخلها.

أما المادة (22) فقد نصت على أنه يعتبر مرتكباً جناية كل شخص يقوم عن عمد أو بإهمال جسيم وبدون وجه حق بإدخال فيروس حاسوبي أو يسمح بذلك في أي حاسوب أو منظومة حاسوب، أو شبكة حاسوب.

كما جاءت المادة (23) لتجريم إلحاق الضرر بالبيانات الحاسوبية بالمسح أو التحوير أو الكتمان.

ونصت المادة (25) على أنه يعتبر مرتكباً جناية أي شخص يقوم عن عمد وبدون وجه حق وبقصد الغش بإدخال بيانات حاسوبية أو تحويرها أو محوها وينتج عنها بيانات غير صحيحة بقصد اعتبارها معلومات صحيحة.

كما نصت المادة (28) على العقوبات المترتبة على التجاوزات التي حددها النظام[1].

كما يجري العمل لإعداد نظام الاختراقات الإلكترونية، الذي يحدد العقوبات المترتبة على الاختراقات الإلكترونية، وتقوم بإعداده وزارة الداخلية للتصدي لمخترقي شبكة المعلومات في المملكة، ويشمل هذا النظام تحديد الجناة القائمين بالاختراق سواء كانوا أفراداً، أو مؤسسات، وكذلك العقوبات النظامية التي يتم تطبيقها بحقهم [2].

---

(1) انظر: مشروع نظام المبادلات الإلكترونية والتجارة الإلكترونية، في المملكة العربية السعودية 1423/3/17هـ، إعداد: وزارة التجارة، إدارة التجارة الإلكترونية. مصادر الحق في الفقه الإسلامي، للدكتور / عبدالرزاق بن أحمد السنهوري، منشورات الحلبي الحقوقية، بيروت، لبنان، الطبعة الثانية، عام 1998م، 44/1.

(2) الأحكام الفقهية للتعامل بالإنترنت، للدكتور محمد داود بكر، ندوة دلة البركة التاسعة عشرة للاقتصاد الإسلامي - مكة المكرمة 1421هـ، ص16.جريدة المدينة، العدد: 14489، 1423/10/20هـ، ص17.

قرار مجلس الوزراء رقم (163) في 1417/10/24هـ:

الذي ينص على إصدار الضوابط المنظمة لاستخدام شبكة الإنترنت والاشتراك فيها، ومن ذلك:

- الامتناع عن الوصول أو محاولة الوصول إلى أي من أنظمة الحاسبات الآلية الموصولة بشبكة الإنترنت، أو إلى أي معلومات خاصة، أو مصادر معلومات دون الحصول على موافقة المالكين، أو من يتمتعون بحقوق الملكية لتلك الأنظمة والمعلومات أو المصادر.
- الامتناع عن استخدام الشبكة لأغراض غير مشروعة، ومن ذلك على سبيل المثال لا الحصر: الرذيلة والقمار، أو القيام بأي نشاطات تخالف القيم الاجتماعية والثقافية والسياسية والإعلامية والاقتصادية والدينية للمملكة العربية السعودية.
- الامتناع عن الإخلال بأي من حقوق النشر أو التأليف، أو حقوق الملكية الفكرية لأي معلومات أو مصادر.
- الامتناع عن إرسال أو استقبال معلومات مشفرة إلا بعد الحصول على التراخيص اللازمة من إدارة الشبكة المعنية.
- الامتناع عن الدخول إلى حسابات الغير، أو محاولة استخدامها بدون تصريح.
- الامتناع عن إشراك الغير في حسابات الاستخدام، أو إطلاعه على الرقم السري للمستخدم.
- الالتزام باحترام الأنظمة الداخلية للشبكات المحلية والدولية عند النفاذ إليها.
- الامتناع عن تعريض الشبكة الداخلية للخطر وذلك عن طريق فتح ثغرات أمنية عليها.

- الامتنـاع عـن الاسـتخدام المكثـف للشـبكة بمـا يشـغلها دومـاً، ويمنـع الآخريـن مـن الاسـتفادة مـن خدماتهـا.

- الالتـزام بمـا تصدره وحـدة خدمـات (الإنترنـت) بمدينـة الملـك عبـد العزيـز للعلـوم والتقنيـة مـن ضوابـط وسياسـات لاسـتخدام الشـبكة.

نـص القـرار عـلى تكويـن لجنـة دائمـة برئاسـة وزارة الداخليـة وعضويـة وزارات الدفـاع، والماليـة، والإعـلام، والـبرق والبريـد والهاتـف والتجـارة، والشـؤون الإسـلامية، والتخطيـط، والتعليـم العـالي والمعـارف، ورئاسـة الاسـتخبارات، ومدينـة الملـك عبـد العزيـز للعلـوم والتقنيـة[1]، وذلـك لمناقشـة مـا يتعلـق بمجـال ضبـط واسـتخدام (الإنترنـت) والتنسـيق فيـما يخـص الجهـات التـي يـراد حجبهـا، ولهـا عـلى الأخـص مـا يـلي:

- الضبـط الأمنـي فيـما يتعلـق بالمعلومـات الـواردة أو الصـادرة عـبر الخـط الخارجـي للإنترنـت والتـي تتنـافى مـع الديـن الحنيـف والأنظمـة[2].

- التنسـيق مـع الجهـات المسـتفيدة مـن الخدمـة فيـما يتعلـق بـإدارة وأمـن الشـبكة الوطنيـة.

مـع التوجـه المتنامـي نحـو تقنيـة المعلومـات، تـبرز بوضـوح الحاجـة الملحـة إلى إيجـاد أنظمـة لضبـط التعامـلات الإلكترونيـة بكافـة صورهـا، فبالرغـم مـن محدوديـة مـا أنجـز في هـذا السـياق فـإن الجهـات التـي تضطلـع بهـذه المهـام تعـاني مـن البـطء الشـديد في إنجـاز هـذه الأنظمـة لكـثرة الجهـات الممثلـة في لجـان الصياغـة،

---

(1) انظر: خصوصية التعاقد عبر الإنترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، تأليف د/ أسامة أبو الحسن مجاهد ص32-34. انظر: مصادر الحق في الفقه الإسلامي، د/ عبد الرزاق أحمد السنهوري، منشورات الحلبي الحقوقية بيروت لبنان، 1998م، الطبعة الثانية، 75/2.

(2) انظر: بحث الدكتور علي القرداغي، مجلة مجمع الفقه الإسلامي - العدد السادس،ج2 1410-هـ ص949.انظر: الأحكام الفقهية للتعامل بالانترنت- د/ محمد داود بكر، بحث مقدم لندوة البركة التاسعة عشرة للاقتصاد الإسلامي - مكة المكرمة، 7-8 رمضان 1421هـ.

وتعـدد الجهـات المرجعيـة التـي تقـوم بمراجعـة الأنظمـة واعتمادهـا، لـذا فـلا بـد مـن إعـداد الأنظمـة اللازمـة لتحقيـق الاسـتفادة القصـوى مـن تقنيـة المعلومـات، وحمايـة المتعاملـين مـن المخاطـر التـي تنطـوي عليهـا تلـك التقنيـات، ولقـد أظهـرت إحصائيـة مـدى الحاجـة إلى وجـود تنظيـمات ولوائـح تحكـم قضايـا تقنيـة المعلومـات أن 70% يـرون الحاجـة إلى ذلك[1].

وعـلى مسـتوى دول العـالم ومـع مواكبـة التطـور الهائـل لتقنيـة المعلومـات تـم إدراج أنظمـة لضبـط التعامـلات الإلكترونيـة، وتضمنـت تلـك الأنظمـة عقوبـات للمخالفـين في التعامـل الإلكـتروني.

ففـي ماليزيـا: صـدر نظـام في عـام 1997م للمخالفـات الإلكترونيـة، وقـد صنـف المخالفـات إلى: الوصـول غـير الشرعـي إلى الحاسـب الآلي والدخـول بنيـة التخريـب أو التعديـل غـير المسـموح بـه، وتـتراوح العقوبـات المحـددة بـين غرامـات ماليـة تصـل إلى 150.000 دولار ماليـزي[2]، مـع السـجن إلى مـدة عـشر سـنين.[3]

وفي أيرلنـدا: صـدر نظـام في عـام 2001م، للحمايـة مـن الجرائـم المعلوماتيـة يتيـح معاقبـة الاسـتخدام غـير المسـموح بـه لأجهـزة وأنظمـة الحاسـب الآلي.

وفي مـصر: يجـري العمـل في وزارة الاتصـالات والمعلومـات لإصـدار نظـام عـن الجريمـة الإلكترونيـة يتضمـن عقوبـات رادعـة لمـن يقـوم مـن الأفـراد

(1) انظر: دراسة الوضع الراهن في محور أحكام في المعلوماتية، ص13.

(2) انظر: دراسة تجارب الدول في مجال أحكام في المعلوماتية، إعداد: د/ محمد القاسم،د/رشيد الزهراني عبد الرحمن السند، عاطف العمري، مشروع الخطة الوطنية لتقنية المعلومات 1423/11/10هـ

(3) قمت بزيارة لماليزيا للاطلاع على التجربة الماليزية الرائدة في مجال تقنية المعلومات في شهر شعبان من عام 1423هـ، ورأيت التطور المبهر الذي وصلت إليه ماليزيا، حتى أصبحت من مصدري التقنية للدول الأخرى، وأصبح دخل ماليزيا من تصدير التقنية يزيد على 100 مليار دولار سنوياً.

أو المؤسسات بتزوير أو إفساد مستند إلكتروني على الشبكة أو الكشف عن بيانات ومعلومات بدون وجه حق، وغيرها من صور الجريمة الإلكترونية.

أما في الأردن: فتم إعداد تنظيم يتعلق بخصوصية المعلومات وسريتها، للمحافظة عليها في ظل التعاملات الإلكترونية عبر الشبكات العالمية للمعلومات، كما ساهمت الأردن في إعداد قانون مكافحة جرائم تقنية المعلومات وما في حكمها والمقدم إلى الإدارة العامة للشؤون القانونية في جامعة الدول العربية [1].

ولقد سعت إمارة دبي بالإمارات العربية المتحدة: إلى التحول الكامل إلى الحكومة الإلكترونية لتكون جميع الإدارات الحكومية متواجدة على الإنترنت ولقد حدد الإطار القانوني لمدينة دبي للإنترنت الحماية الكاملة للمعلومات وخصوصيتها وحماية حقوق الملكية الإبداعية، ورقابة الجريمة المرتبطة بالتعاملات الإلكترونية.

صعوبة التعاون الدولي في مكافحة الجريمة الإلكترونية:

في عالم مزدحم بشبكات اتصالات دقيقة تنقل وتستقبل المعلومات من مناطق جغرافية متباعدة باستخدام تقنيات لا تكفل للمعلومات أمناً كاملاً، يتاح في ظلها التلاعب عبر الحدود بالبيانات المنقولة أو المخزنة، مما قد يسبب لبعض الدول أو الأفراد أضراراً فادحة، يغدو التعاون الدولي واسع المدى في مكافحة الجرائم الواقعة في بيئة المعالجة الآلية للبيانات أمراً متحتماً، ومع الحاجة الماسة لهذا التعاون إلا أن عقبات عدة تقف في سبيله أبرزها ما يلي:

---

(1) انظر: خصوصية التعاقد عبر الإنترنت ص107، وانظر: العقود الإلكترونية، عبد الوهاب بدري – مجلة عصر الحاسب، تصدر عن جمعية الحاسبات السعودية – العدد الخامس، عام 2001م، ص52. انظر: النظام القانوني لحماية التجارة الإلكترونية، د/ عبد الفتاح بيومي حجازي، دار الفكر الجامعي الإسكندرية، الطبعة الأولى عام، 2002م، 118/1. النظام القانوني لحماية التجارة الإلكترونية، د/ عبد الفتاح بيومي حجازي، دار الفكر الجامعي الإسكندرية، الطبعة الأولى عام، 2002م، 118/1.

- عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات الواجب تجريمها.

- عدم الوصول إلى مفهوم عام موحد حول النشاط الذي يمكن الاتفاق على تجريمه.

- اختلاف مفاهيم الجريمة باختلاف الحضارات.

- عدم وجود معاهدات دولية لمواجهة المتطلبات الخاصة بالجرائم الإلكترونية.

- تعقد المشاكل النظامية والفنية الخاصة بتفتيش نظام معلوماتي خارج حدود الدولة، أو ضبط معلومات مخزنة فيه، أو الأمر بتسليمها.

وسعياً للتغلب على هذه المشكلات أو بعضها، أهاب مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين والذي عقد في هافانا، في قراره المتعلق بالجرائم ذات الصلة بالحاسب الآلي[1]، بالدول الأعضاء أن تكثف جهودها كي تكافح بمزيد من الفعالية عمليات إساءة استعمال الحاسب الآلي التي تستدعي تطبيق جزاءات جنائية على الصعيد الوطني، بما في ذلك النظر إذا دعت الضرورة في:

---

(1) انظر: الحماية الجنائية الخاصة – دراسة مقارنة – د/ أسامة قايد، دار النهضة العربية، القاهرة، عام 1994م ص41.انظر: الحماية الجنائية للتجارة الإلكترونية، د/ مدحت عبد الحليم رمضان، دار النهضة العربية، القاهرة عام 2001م، ص102.الحكومة الإلكترونية – مسرح الجريمة -، د/ عبد القادر الفنتوخ، جريدة الرياض، العدد: 12312، الأحد 26 / 12 / 1422هـ، ص41.انظر: التهديدات الإجرامية للتجارة الإلكترونية، د/ سهير حجازي، مركز البحوث والدراسات، شرطة دبي، دولة الإمارات العربية المتحدة، العدد (91). الاختراقات الإلكترونية خطر كيف نواجهه، موزة المزروعي، مجلة آفاق اقتصادية، دولة الإمارات العربية المتحدة، العدد التاسع، سبتمبر 2000م، ص54.انظر: جرائم استخدام شبكة المعلومات العالمية – الجريمة عبر الإنترنت، د/ ممدوح عبد الحميد عبد المطلب بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة ص7.وانظر: التدمير المتعمد لأنظمة المعلومات الإلكترونية، د/عبادة أحمد عبادة، مركز البحوث والدراسات بشرطة دبي الإمارات العربية المتحدة، مارس 1999م، ص2.

- تحديث الأنظمة والإجراءات الجنائية بما في ذلك اتخاذ تدابير من أجل ضمان أن تكون الجزاءات بشأن سلطات التحقيق وقبول الأدلة على نحو ملائم.
- النص على جرائم وجزاءات وإجراءات تتعلق بالتحقيق والأدلة، للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي.

كما حث المؤتمر الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالحاسبات، بما في ذلك دخولها حسب الاقتضاء أطرافاً في المعاهدات المتعلقة بتسليم المجرمين، وتبادل المساعدة الخاصة المرتبطة بالجرائم ذات الصلة بالحاسب الآلي، وأن يسفر بحث مؤتمرات الأمم المتحدة لموضوع الجرائم ذات الصلة بالحاسب عن فتح آفاق جديدة للتعاون الدولي في هذا المضمار لاسيما فيما يتعلق بوضع أو تطوير ما يلي:

- معايير دولية لأمن المعالجة الآلية للبيانات.
- تدابير ملائمة لحل مشكلات الاختصاص القضائي التي تثيرها الجرائم المعلوماتية العابرة للحدود، أو ذات الطبيعة الدولية.
- اتفاقيات دولية تنطوي على نصوص تنظيم إجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها، والأشكال الأخرى للمساعدة المتبادلة، مع كفالة الحماية في الوقت نفسه لحقوق الأفراد والدول [1]

---

(1) انظر: الجرائم المعلوماتية، أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي، د/ هشام محمد فريد رستم، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، الذي نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، 2000م، ص48،49. التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الإنترنت، عماد علي الخليل، عمان الأردن، عام 2000م، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، ص4.التكنولوجيا الحديثة والاتصال الدولي والإنترنت، د/ علي محمد شمر، الشركة السعودية للأبحاث والنشر، جدة، المملكة العربية السعودية، 1997م، ص244.

جرائـم إلكترونية تمـت المعاقبة عليها:

نـشر مؤخـراً خـبر عـن صـدور حكـم في بريطانيـا بالسـجن لمـدة عامـين ضـد أحـد قراصنـة الإنترنـت الـذي قـام بإنتـاج وتوزيـع أخطـر أنـواع فيروسـات الحاسـب في العـالم والتـي كان يرسـلها عـلى شـكل رسـائل غراميـة، أو تحذيـرات أمنيـة أحيانـاً، وتعـد الفيروسـات التـي قـام بإنتاجها وتوزيعهـا في المرتبـة الثانيـة في قائمـة الفيروسـات الأكـثر انتشـاراً في العـالم، وقـد وصلـت التقديـرات الخاصـة بتكلفـة تنظيـف الأجهـزة المصابـة بهـذه الفيروسـات إلى ملايـين الـدولارات، وقـد ألقـي القبـض عـلى المخـرب (فالـور) الـذي يعتـبر مـن أكـبر مصممـي شـبكات المعلومـات في العـالم، وهـو يتفاخـر بهـذه الأعـمال عـبر غـرف الدردشـة عـلى شـبكة المعلومـات العالميـة، وقـد قـام بإنشـاء وتوزيـع الفيروسـات خـلال الفـترة مـن ديسـمبر 2001م إلى ينايـر 2002م [1].

(1) انظر: موقف الشريعة الإسلامية من جرائم الحاسب الآلي والإنترنت، عطا عبد العاطي محمد السنباطي دار النهضة العربية، القاهرة، الطبعة الأولى، 1422هـ، ص33.الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، د/ عبد الفتاح بيومي حجازي، دار الكتب القانونية، مصر، 2002م، ص68. الحماية الجنائية للبيانات المعالجة إلكترونياً، د/ علي بن عبد القادر القهوجي، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، عام2000م. الحماية الجنائية للبيانات المعالجة إلكترونياً.جريدة الرياض، العدد: 12632، يوم الجمعة 28 / 11 / 1423هـ، ص46.

المطلب الثاني

المراقبة التقنية

منذ أول حالة لجريمة موثقة ارتكبت عام 1958م في الولايات المتحدة الأمريكية بواسطة الحاسب الآلي وحتى الآن كبر حجم هذه الجرائم وتنوعت أساليبها وتعددت اتجاهاتها وزادت خسائرها وأخطارها، حتى صارت من مصادر التهديد البالغة للأمن القومي للدول، خصوصاً تلك التي ترتكز مصالحها الحيوية على المعلوماتية، وتعتمد عليها في تسيير شئونها، فقد تحولت هذه الجرائم من مجرد انتهاكات فردية لأمن النظم والمعلومات إلى ظاهرة تقنية عامة، ينخرط فيها الكثير ممن تتوافر لديهم القدرات في مجال الحاسب الآلي والاتصال بشبكات المعلومات.

وتتم المراقبة التقنية بعدة وسائل منها:

أولاً: تشفير البيانات المهمة المنقولة عبر الإنترنت.

ثانياً: إيجاد نظام أمني متكامل يقوم بحماية البيانات والمعلومات.

ثالثاً: توفير برامج الكشف عن الفيروسات والمقاومة لها لحماية الحاسب الآلي والبيانات والمعلومات من الإضرار بها.

رابعاً: عدم استخدام شبكات الحاسب الآلي المفتوحة لتداول المعلومات الأمنية، مع عمل وسائل التحكم في الدخول إلى المعلومات والمحافظة على سريتها[1].

---

(1) الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني، د/ هدى حامد قشقوش، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، عام 2000م ص13.فكرة الحماية الجنائية لبرامج الحاسب الآلي، للدكتور / محمد محمد شتا، دار الجامعة الجديدة للنشر الإسكندرية، 2001م، ص22.

خامساً: توزيع مهام العمل بين العاملين، فلا يعطى المبرمج مثلاً وظيفة تشغيل الحاسب الآلي إضافة إلى عمله، ففي هذه الحالة سوف يكون قادراً على كتابة برامج قد تكون غير سليمة، ومن ثم تنفيذها على البيانات الحقيقية، كما يتم توزيع مهام البرنامج الواحد على مجموعة من المبرمجين، مما يجعل كتابة برامج ضارة أمراً صعباً.

المطلب الثالث

التدريب والتأهيل

تتطلب مواجهة الاعتداءات الإلكترونية تدريب الكوادر القادرة على مواجهة تلك الاعتداءات، وفي البداية حتى يؤتي التدريب ثماره لابد أن تتوافر لدى المتدرب الصلاحية العلمية والقدرات الذهنية والنفسية لتلقي التدريب، بل يقرر بعض الخبراء أنه لا بد أن تتوافر فيمن يتلقى التدريب الخبرة الكافية في المجالات المرتبطة بعمليات الحاسب، والبرمجة، وتصميم النظم وتحليلها، ومن الأهمية بمكان أن يتضمن البرنامج التدريبي في التحقق من الجرائم الإلكترونية سائر المجالات الحيوية للمعرفة، إضافة إلى محاضرات ودراسة حالات، ونقل خبرات علمية في مختلف جوانب عمليات الحاسب الآلي وشبكات المعلومات.

والموضوعات التي ينبغي أن يتضمنها البرنامج التدريبي يمكن إيجازها فيما يأتي:

1. أنواع المخاطر والتهديدات ونقاط الضعف التي يكون الحاسب أو شبكة المعلومات قابلاً للتعرض لها.
2. مفاهيم معالجة البيانات سواء ما يتعلق منها بالبرامج أو الأجهزة.
3. أنواع الجرائم الناشئة عن إساءة استخدام الحاسب الآلي أو شبكات المعلومات.
4. أساسيات الحاسب الآلي، والمعالجة الإلكترونية للبيانات، وأمن الحاسب وشبكات المعلومات، والجريمة المعلوماتية، والإثبات الإلكتروني.

والتدريـب على مواجهـة الجرائم المعلوماتيـة يمكن بطريقين:

الأول: التدريـب أثنـاء الوظيفـة بـأن يتلقـى الفـرد هـذا النـوع مـن التدريـب عــن طريــق تكليفــه بالعمــل مــع شــخص لديــه خــبرة في مواجهــة الجرائــم المعلوماتيــة.

والثـاني: التدريــب مــن خــلال حلقــات دراســية، وحلقــات نقــاش، أو مــا يسـمى بـورش العمـل، تعقـد حـول جرائـم الحاسـب، وأمـن الحاسـب والشـبكات وتتضمـن نقاشـات المشـاركين، وخـبراء الحاسـب المتخصصـين في المعالجـة الإلكترونيـة للبيانـات بالإضافـة إلى رجـال الشرطـة الذيـن تـوكل إليهـم مهمـة القبـض عـلى مرتكبـي هـذه الجرائـم[1].

إن الجرائــم المعلوماتيــة تنفــرد عــن غيرهــا مــن صــور الجرائــم الأخــرى بخصائـص معينـة ترجـع إلى طبيعتهـا الخاصـة ومـا يكتنفهـا مـن خطـوات فنيـة، لـذا كان إجـراء تحقيقـات ناجحـة فيهـا يقتـضي تلقـي معـارف وتدريـب خـاص يكفـلان لمحققـي الشرطـة وممثـلي الادعـاء العـام اكتسـاب مهـارات حقيقيـة متطـورة تلائـم هـذا النـوع مـن الجرائـم لاسيما فيـما يتعلـق بالمحافظـة عـلى حقـوق جميـع الأطـراف في الدعـوى والسـيطرة عـلى التحقيـق وتوجيهـه بمعاونـة الخـبراء والفنيـين، ولذلـك فـإن تخلـف خطـط وبرامـج تأهيـل وتدريـب الشرطـة وأجهـزة التحقيـق والادعـاء، ومـا ينجـم عنهـا مـن نقـص أو انعـدام مواكبـة التطـور المتلاحـق والسريـع لتقنيـات المعلومـات واسـتخداماتها الإجرائيـة موضـع إجـماع في المؤتمـرات الدوليـة التـي تعقـد حـول التحقيـق الجنـائي [2].

(1) انظر: الجرائم المعلوماتية، أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي، د/ هشام محمد فريد رستم، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، الذي نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، 2000م، ص48،49.

(2) انظر: الجرائم المعلوماتية (أصول التحقيق الجنائي الفني)، ص120 وما بعدها.

لقد سعت الدول إلى إقامة دورات متخصصة في الجرائم المعلوماتية.

وفي المملكة العربية السعودية: التي تسعى للدخول في التجارة الإلكترونية بشكل واسع عبر معالجة المعوقات التي تحد من ذلك ومنها الجرائم الإلكترونية، بدأت في عقد دورات تدريبية، هي الأولى من نوعها، حول موضوع مكافحة جرائم الحاسب الآلي بمشاركة مختصين دوليين، وتقدر تكلفة جرائم الحاسب الآلي في منطقة الشرق الأوسط بحوالي 600 مليون دولار، 25% من هذه الجرائم تعرض لها أفراد ومؤسسات من السعودية خلال عام 2000م فقط، وفيما تعمل لجنة سعودية حكومية مكونة من وكلاء الوزارات المعنية بهذا الموضوع على الانتهاء من إنجاز مشروع نظام التجارة الإلكترونية، فهي مكلفة أيضاً بوضع النظم والبيانات، وتقييم البنية التحتية، وطاقة العناصر المتعلقة بالتعاملات الإلكترونية، وتأتي هذه الاستعدادات للحد من انتشار هذا النوع من الجريمة محلياً بعد فتح باب التجارة الإلكترونية فيها، خاصة أن العالم يعاني من انتشارها بشكل واسع، بعد أن تطورت بشكل لافت للنظر فيما يخص ماهية هذا النوع من الجرائم، ومرتكبيها، وأنواعها ووسائل مكافحتها إلى جانب الأحكام والأنظمة التي تحد من ارتكابها.

وتهدف الإجراءات في المملكة العربية السعودية: إلى تنمية معارف ومهارات المشاركين في مجال مكافحة الجرائم التي ترتكب بواسطة الكمبيوتر، أو عبر شبكة الحاسب الآلي وتحديد أنواعها ومدلولاتها الأمنية، وكيفية ارتكابها، وتطبيق الإجراءات الفنية لأمن المعلومات في البرمجيات، وأمن الاتصالات في شبكات الحاسب الآلي والإجراءات الإدارية لأمن استخدام المعلومات، ويرتكب هذا النوع من الجرائم بواسطة عدة فئات مختلفة، منها فئة الهواة، وغالبية هؤلاء من المراهقين، الذين يرتكبون جرائم الكمبيوتر من أجل قهر النظام، وكسر الحواجز الأمنية.

وقد سجلت سوابق أمنية لأشخاص استخدموا أجهزة الكمبيوتر في

الدخـول إلى شـبكات المعلومـات الاسـتراتيجية المسـتخدمة لـدى الجهـات الأمنيـة والعسـكرية بغـرض الاطـلاع عليهـا والتلاعـب بمحتوياتهـا، ولعـل الفئـة الأخطـر مـن مرتكبـي هـذا النـوع مـن الجرائـم هـي فئـة الجريمـة المنظمـة، التـي يسـتخدم أفرادهـا الحاسـب الآلي لأغـراض السرقـة أو السـطو عـلى المصـارف والمنشـآت التجاريـة، بمـا في ذلـك سرقـة أرقـام البطاقـات الائتمانيـة والأرقـام السريـة ونشرهـا أحيانـاً عـلى شـبكة الإنترنـت كـما تسـتخدم هـذه الفئـة الحاسـب الآلي لإدارة أعمالهـا غـير المشروعـة كالقـمار والمخـدرات وغسـيل الأمـوال، ورغـم تنـوع الفئـات التـي ترتكـب هـذه النوعيـة مـن الجرائـم إلا أن الطـرق المسـتخدمة في الجريمـة تتشـابه في أحيـان كثـيرة ولذلـك فـإن أجهـزة الأمـن بحاجـة إلى الكثـير مـن العمـل لتطويـر قدراتهـا للتعامـل مـع جرائـم الكمبيوتـر، وخاصـة في مـسرح الجريمـة، حتـى يكـون رجـل التحقيـق قـادراً عـلى التعامـل مـع الأدوات الإلكترونيـة مـن أجهـزة وبرامـج[1].

في الولايـات المتحـدة: وهـي أول دولـة في العـالم عنيـت بتوفـير التدريـب الـلازم لمكافحـة الجرائـم المعلوماتيـة والتحقيـق فيهـا مـن خـلال دورات متخصصـة تعقدهـا أكاديميـة مكتـب التحقيقـات الفيدراليـة لتزويـد محققـي الشرطـة والعاملـين في الإدارات الجنائيـة بمعـارف ومهـارات حـول برمجـة الحاسـب وتشـغيله، مـع اسـتخدام تطبيـق بنـكي مصغـر وحاسـب آلي، وذلـك في إطـار حملـة تدريبيـة تقـوم عـلى رفـع نسـبة المعرفـة بالحاسـبات بـين القائمـين عـلى تنفيـذ الأنظمـة في البـلاد، فبعـد تصاعـد موجـة الاعتـداء عـلى مواقـع الإنترنـت لـشركات أمريكيـة كـبرى، اعتـبرت وزارة العـدل الأمريكيـة ومكتـب التحقيقـات الفيـدرالي أنهـما ملتزمـان بملاحقـة المسـئولين عـن هـذه الأعـمال والتأكـد مـن تنفيـذ العقوبـات عليهـم حتـى تظـل شـبكة الإنترنـت بيئـة آمنـة لممارسـة الأعـمال والتجـارة الإلكترونيـة.

---

(1) انظر: السعودية تعقد دورات لمكافحة جرائم الكمبيوتر بعد خسائر تقدر بأكثر من 150 مليون دولار لحقت بمؤسساتها الوطنية، عمر الزبيدي، جريدة الشرق الأوسط، العدد: 8196، يوم الاثنين 2001/5/7م، ص15.

واعتبرت الحكومة الأمريكية هذه الاعتداءات هجوماً على المصالح الأمريكية لحرمانها من عائدات الإنترنت [1].

ولكيلا تتخلف أجهزة الشرطة وجهات القبض والتحقيق عن مواكبة تيار التقدم المتوالي في مجال تقنيات الحاسبات والمعلوماتية، وتتأخر عن ملاحقة متغيراته فيتدهور مستوى قدراتها عن أداء واجبها في الذود عن المجتمع ضد هذا النوع من الجرائم الفنية، ووصولاً بالمواجهة الفاعلة لهذه الجرائم إلى أقصى درجات الكفاءة والفعالية يوصى بالآتي:

- إنشاء جهاز أو إدارة فنية متخصصة تتولى مهمة الاستقصاء والتحري وعمليات البحث الجنائي والتحقيق الفني وجمع الأدلة في الجرائم المعلوماتية وتزويدها بالأجهزة والمعدات الفنية المتطورة اللازمة لنجاح عملها وبمحققين وفنيين تتوافر فيهم الصلاحية العلمية والكفاءة الفنية، والصفات الشخصية المطلوبة للقيام بهذه المهام.
- تبني خطة تدريبية تكفل لجهاز الشرطة والجهات الأخرى ذات العلاقة رفع المعرفة بتقنيات الحاسبات والمعلومات، وطرق وكيفية إساءة استخدامها في ارتكاب الجرائم بما يكفل التصدي لجرائم المعلوماتية.
- استحداث برامج تدريبية تخصصية تكفل توافر العنصر البشري المدرب والمؤهل لاستيعاب معطيات ومنجزات الثورة المعلوماتية، واستخدامها والإفادة منها في كشف غموض الجرائم التي تقع باستخدام تقنياتها والقادر كذلك على مواكبة متغيراتها التي يمكن أن تستخدم في ارتكاب الجريمة وإعداد الوسائل المناسبة للوقاية منها ومكافحتها.

---

(1) انظر: الجرائم المعلوماتية، د/ هشام محمد فريد رستم، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت ص122.

- الاستفادة من طرق وأساليب مرتكبي الجرائم الإلكترونية، ومعرفة خططهم وذلك عند القبض عليهم واكتشافهم، ومحاولة معرفة الثغرات الأمنية والفنية التي استفادوا منها في تنفيذ اعتدائهم، حتى يمكن تلافيها مستقبلاً.

- جمع وتصنيف حالات الإجرام المعلوماتي في الأقطار العربية وغيرها وإعداد دراسة متكاملة عن تلك الحالات، ويتم استخدامها ضمن أساليب تدريب محققي الجرائم المعلوماتية في دورات تعقد وفقاً لاحتياجاتها.

- تبادل المعلومات والخبرات المتعلقة بالإجرام المعلوماتي مع الأجهزة البحثية المعنية به، وأجهزة المكافحة، للوصول إلى معرفة الأساليب والدوافع والطرق والأساليب المتبعة في مثل هذا النوع من الجرائم، مع دراسة أبرز أشكال هذه الجرائم وحجمها واتجاهاتها، واستشراف مستقبلها، ووضع تصور للوقاية منها ومكافحتها[1].

(1) انظر: الجرائم المعلوماتية د/ هشام محمد فريد رستم، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، ص127.

الفصل الثانى

المسؤولية الجنائية لمتعهدى الإيواء

مع نهايات القرن العشرين شهد العالم، وبشكلٍ لم يسبق له مثيل، تطوراً هائلاً ومتسارعاً في عالم الاتصالات وتكنولوجيا المعلومات، ونتيجة لهذه التطورات التكنولوجية وما صاحبها من تقدم في صناعة الحاسبات الآلية، بدا العالم كقرية صغيرة ذابت فيه الحواجز، فتداخل وتشابك وارتبط سكانه بشبكة عنكبوتية عالمية يسبح فيها الجميع بحريَّة، فإذا بها ثورة المعلوماتية، إنعكس آثارها علي كافة الأصعدة والميادين ومنها الثقافية، والاقتصادية، والإجتماعية....[1]

وأمام هذا التقدم العلمي والتكنولوجي، وفي ظلٍّ غزوِ شبكة الإنترنت لكافة مناحي الحياة، ولاشك أن ذلك كان له أكبر الأثر، وبخاصة ما حدث مؤخرا من أنه كان البيئة التي أثمرت هذا الربيع العربي، وبزغت بوادر الخير لفتحِ آفاقٍ جديدة لتقدم البشريَّة ولجني ثمار التواصل والمعرفة، إلاَّ أنه،

(1) Adsit، C. Kristin. (1999). Internet Pornography Addiction.[Online].Available: http://www.chemistry.vt.edu/chem-dept/ dessy/honors /papers99/adsit.htm [9.3.2001]. Highley، Reid. (1999). Viruses: The Internet's Illness.[Online]. Available:http://www.chemistry.vt.edu/chem-dept/dessy/honors /papers99/highleh.htm [9.3.2001].

ظهرت في نفس الوقت نوازع الشر لاستغلال هذا التقدم لتحقيق أغراضٍ شخصية على حساب قيم المجتمع[1]، وحقوق الأفراد والجماعة وأمنهم، فما كان من أصحاب النفوس الضعيفة، أو من عصابات الجريمة المنظمة، أو من يستتر من خلالها لتحقيق أغراض مختلفة منها، ما هو سياسي أو أخلاقي..، إلاَّ أنهم تجرَّؤوا على إستغلال شبكة الإنترنت فحولها إلى مسرحٍ يرتكبون فيه العديد من الجرائم والمخالفات: فقاموا بنشر الأخبار المزيَّفة[2]، وبثوا الأفكار والممارسات المناهضة للأديان السماوية وللإنسانية، ونشروا الصور الفاضحة للصغار قبل الكبار، وانتهكوا حرمة الحياة الخاصة لأفراد المجتمع، وحملوا أو شهروا بالأشخاص أو قذفهوهم، وتعدُّوا على حقوق الملكية الفكرية... وما هذه إلاَّ نماذج من سلسلة مخالفات تُرتكب عبر الإنترنت يصعب حصرها.

والواقع العملي يُثبت أن تداول المعلومات عبر شبكة الإنترنت بحاجة إلى تظافر جهود الأشخاص القائمين على إدارتها[3]، والذين تتنوَّع أدوارهم وأنشطتهم في تشغيلها، فحتى يتمكن مستخدمو الإنترنت من الدخول إلى الشبكة، والإبحار فيها بحرِّية، والوصول إلى ما يصبون إليه من معلومات أو بثِّها، لا بُدَّ من وجود عدَّة أشخاص أو وسطاء، يُطلق عليهم عادةً مصطلح"مقدمي خدمات الإنترنت"، أو"الوسطاء في خدمات الإنترنت"، يتولُّون عملية إيواء المعلومات، وبثِّها، وعرضها[4].

---

(1) Koerner، B. I. (1999،November 22). Only you can prevent computer intrusions. U.S. News and World Report، 127، pp. 50. Morningstar، Steve. (1998). Internet Crime and Criminal Procedures. [Online]. Available: http://www.prevent-abuse-now.com/index.html [13.10.2001].

(2) في المسؤولية الإلكترونية بشكلٍ عام عن المخالفات المرتكبة عبر الإنترنت، راجع، محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، الطبعة الأولى، 2003.

(3) تعتبر الصين ثاني أكبر سوق للانترنت في العالم وذلك بوجود نحو 843 ألف موقع الكتروني، ويصل مستخدمي الانترنت فيها إلى نحو 140 مليون شخص، راجع سناء عيسى - مقال بعنوان فيروسات جديدة تستهدف أنظمة مايكروسوفت- مجلة العالم الرقمي- العدد 38 بتاريخ 2003/09/14 منشورة على الموقع الالكتروني www.al-jazirah.com

(4) في تعدُّد أشخاص القائمين على خدمات الإنترنت، انظر: عبد الفتاح بيومي حجازي،=

وهـذا التنـوُّع في أدوارهـم والتعـدُّد في أنشـطتهم يجعـل مـن اليسـير عليهـم تتبُّـع النشـاط المعلومـاتي غـير المـشروع وكشـفه، وبخاصـة أنهـم القائمـون عـلي إدارة مـا يحـدث مـن خـلال المجـال المتـاح لجمهـور المتعاملـين، كـما ان لديهـم في أحيـان كثـيرة القـدرة عـلي التعـرض للخصوصيـة لطالبـي الخدمـة، إلاَّ أن تحقيـق ذلـك يبقـى رهـن وجـود ضوابـط قانونيـة تُحـدِّد حقـوق أطـراف النشـاط الإلكـتروني والتزاماتـه في مواجهـة بعضهـم البعـض مـن جهـة، وفي مواجهـة المجتمـع الـذي يعيشـون فيـه مـن جهـةٍ أُخـرى، لـذا بـدت الحاجـة ماسـة لإيجـاد تنظيـم تشريعـي متكامـل يُحـدد المركـز القانـوني لمقدمـي خدمـات الإنترنـت، ويُبـين في نفـس الوقـت مسـؤولية كلٍّ منهـم عـمّا يُرتكـب مـن مخالفـات عـبر الشـبكة، الأمـر الـذي لا يُمكـن تحقيقـه إلا بتظافـر جهـود المشرِّعـين عـلى الصعيديـن: الوطنـي والـدولي، وبخاصـة في عـدم وجـود جهـة مرجعيـة لمـا يتـم مـن خـلال الشـبكة المعلوماتيـة ككل.

هـذه الحقيقـة كانـت نـواة عمـل البرلمـان الأُوروبي الـذي تبنَّـى بالإجـماع في 8 يونيـو 2000م التوجيـه رقـم 2000/31، والمتعلِّق"ببعـض الأوجـه القانونيـة لخدمـات شركات المعلومـات، وبصفـةٍ خاصَّـة التجـارة الإلكترونيـة، في السـوق الداخـلي"[1]، والـذي تـمَّ تخصيـص القسـم الرابـع منـه لتنظيـم المركـز القانـوني

= النظام القانوني لحماية الحكومة الإلكترونية، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2003م، ص 339 وما بعدها، محمد حسين منصور، ص 196 وما بعدها،

Lionel THOUMYRE،"Hyper dossier sur les acteurs de l›Internet en France»، juriscom.net، 22 juin 2004، disponible à l›adresse www.juriscom.net /pro/ visu. php? ID = 485.

القانون الفرنسي رقم 2004/575 حول"الثقة في الاقتصاد الرقمي»،

Loi nº 2004575/ du 21 juin 2004 sur la Confiance dans l´économie numérique، JO، 22 juin 2004، p.11168.

(1) التوجيه الأوروبي رقم 2000/31 والمتعلِّق"ببعض الأوجه القانونية لخدمات شركات المعلومات، وبصفةٍ خاصَّة التجارة الإلكترونية، في السوق الداخلي»،

Directive nº 200031//CE du Parlement européen et du Conseil du 8 juin 2000 relative"à certains aspects juridiques des services de la société de l´information، et notamment du commerce électronique، dans le marché intérieur»، JOCE، nº L 178،17 juillet 2000، p.1 ets.

للوسـطاء في خدمـات الإنترنـت، وذلـك عـلى غـرار القانـون الأمريـكي الصـادر في 28 أكتوبـر 1998م للحـد مـن الاعتـداءات عـلى حقـوق الملكيـة الفكريـة في نطـاق الإنترنـت والمسـمَّى بـ Digital Millenium Copyright Act (DMCA)[1]، والـذي خصـص البـاب الثـاني منـه لتحديـد مسـؤولية مقدمـي خدمـات الإنترنـت عـن التعـدي عـلى هـذه الحقـوق.

وقـد جـاءت المـادة (22) مـن التوجيـه الأُوروبي لتلـزم الـدول الأعضـاء في الإتِّحاد الأُوروبي عـلى نقـل أحكامـه إلى تشريعاتهـم الداخليـة بحلـول 17 ينايـر 2002م.

والتزامـاً منهـا بذلـك قدَّمـت الحكومـة الفرنسـية في 14 يونيـو 2001م، كمحاولـةٍ أُولى، مـشروع قانـونٍ حـول"شركات المعلوماتيـة"، والـذي حـدَّدت في قسـمٍ منـه المركـز القانـوني لمـزودي خدمـات الإنترنـت، إلا أن هـذا المـشروع أضحـى لاغيـاً بتغـيُّر المـشِّرع[2].

فجـاءت الحكومـة الفرنسـية مـن جديـد في 15 ينايـر 2003م بمـشروع قانـونٍ حول"الثقـة في الاقتصـاد الرقمـي"، والـذي تـمَّ الموافقـة عليـه مـن قِبـل المـشِّرع الفرنـسي في 21 يونيـو 2004م[3]، واعتبـارا مـن هـذا التاريـخ أصبـح

(1) القانون الأمريكي الصادر في 28 تشرين الأول 1998 والمسمَّى Digital Millenium Copyright Act (DMCA) (Public Law nº 105-304، 112 sat، 2860، 28 oct. 1998.)، يُمكن أيضاً الإطِّلاع على نصوص هذا القانون على الموقع الإلكتروني للمكتب الأمريكي لحقوق النشر وذلك على العنوان التالي:
http://lcweb.loc.gov/copyright.

(2) Luc GRYNBAUM،"LCEN. Une immunité relative des prestataires de services Internet»، Communication- Commerce électronique، Études، Septembre 2004، nº 28، p. 36.

(3) القانون الفرنسي رقم 2004/575 حول"الثقة في الاقتصاد الرقمي»، du 21 juin 2004 sur la Confiance dans l´économie numérique، JO، 22 juin 2004، 575/Loi nº 2004 .p.11168

التوجيه الأوروبي رقم 2000/31 والمتعلِّق"ببعض الأوجه القانونية لخدمات شركات المعلومات، وبصفةٍ خاصَّة التجارة الإلكترونية، في السوق الداخلي»، CE du Parlement européen et/31/Directive nº 2000 du Conseil du 8 juin 2000 relative"à certains aspects juridiques des services de la société de l´information، et notamment du commerce électronique، dans le marché intérieur»، .JOCE، nº L 178،17 juillet 2000، p.1 ets

لمقدمـي خدمـات الإنترنـت في فرنسـا نظامهـم القانـوني الخـاص، وسـنعرض لذلـك مـن خـلال المباحـث التاليـة:

المبحث الأول: المسـئولية المفترضة.

المبحـث الثـاني: الآلية الإجرائية للجريمـة المعلوماتية.

المبحـث الثالث: التعاون الدولي.

المبحث الأول

المسئولية المفترضة

قد تنشأ المسئولية الجنائية نتيجة إسناد فعل ما لشخص، وقد تنشأ المسئولية الجنائية لأسباب أخري، تتمثل في الالتزام القانوني بتحمل التبعة فهي تنشأ تابعة لالتزام آخر وهو في حقيقته واجب اصلي[1].

فللمسؤولية الجنائية ركنان اساسيان:

الاول: هو الرابطة المادية بين الواقعة والنشاط المادي أي الاسناد المادي من جهة.

والثاني: هو الرابطة المعنوية بين الشخص و السلوك.

فاذا كانت القاعدة العامة في أساس المسئولية الجنائية شخصية، و كان كل انسان لا يسأل الا عن اعماله وسلوكه، فإن المشرع المصري اسوة بغيره من مشرعي الأنظمة المقارنة، خرج عن هذه القاعدة واخذ بالمسئولية الجنائية عن الغير في مجال النشر فأخذ بالمسئولية الجنائية المفترضة على اساس تضامني يتمثل في افتراض علم رئيس التحرير بالمضمون المنشور في الصحيفة واعتباره الفاعل الأصلي في الجرائم المرتكبة بواسطة النشر، وهي المسئولية الجنائية المفترضة على أساس تضامني استناد إلى علم رئيس التحرير بالمضمون المنشور في الصحيفة و اعتباره الفاعل الأصلي وكل من يساهم فيها بعد فاعلا او شريكا حسب القواعد العامة بحيث لا يسال شخص بينهم ما دام يوجد

---

(1) د.عبد الله عبد العزيز اليوسف.(1420هـ). التقنية والجرائم المستحدثة، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، تونس (-195 233)

مـن قدمـه عليـه القانـون في ترتيـب المسـئولية الجنائيـة وهـي مـا تسـمى بالمسـئولية المتابعـة أو المسـؤولية المفترضـة أو المسـؤولية الموضوعية...إلـخ[1].

وإن كانـت هنـاك إتجـاه في الفقـه يسـعي إلي إحـلال الغرامـات الماليـة كعقوبـة أصليـة بـدلا عـن العقوبـات السـالبة للحريـة، وهـو إتجـاه محـل نظـر، لأننـا لـو إسـتعرضنا الآثـار السـلبية التـي سـتلحق المجنـي عليـه سـيفوق بكثـير، أي غرامـات ماليـة، مـا لم يطبـق المـشرع المسـؤولية الجنائيـة للشـخص المعنـوي.

ففكـرة المسـئولية المفترضـة تقـوم عـلى ترتيـب الاشـخاص المسـؤولين جنائيـا وحصرهـم بحيـث لا يسـال واحـد منهـم الا اذا لم يوجـد غـيره ممـن قدمـه القانـون عليـه في الترتيـب حتـى نصـل الى دار النـشر أو الطباعـة وهـو مـا نـص عليـه المـشرع المـصري [2]في المـادة 178 مكـرراً (1)إذا ارتكـب الجرائـم المنصـوص عليهـا فى المـادة السـابقة عـن طريـق الصحـف يكـون رؤسـاء التحريـر والنـاشرون مسـئولين كفاعلـين أصليـين بمجـرد النـشر.

وفى جميـع الأحـوال التـي لا يمكـن فيهـا معرفـة مرتكـب الجريمـة يعاقـب بصفتهـم فاعلـين أصليـين الطابعـون والعارضـون والموزعـون.

ويجـوز معاقبـة المسـتوردين والمصدريـن والوسـطاء بصفتهـم فاعلـين

---

(1) د. محمد محمود مندورة. (1410هـ). الجرائم الحاسب الآلية، دورة فيروس الحاسب الآلي، مكتب الأفاق المتحدة: الرياض، 19 – 26.د. عبد المجيد سيد احمد منصور.(1410هـ). السلوك الاجرامي والتفسير الاسلامي. الرياض: مركز ابحاث الجريمة.

(2) من القانون الليبي في المادة 64ع. لعلى أنه (مع مراعاة مسؤولية المؤلف وباستثناء حالات الاشتراك اذا ارتكبت احدى الجرائم عن طريق الصحافة الدورية يعاقب حسب الاحكام الاتية: المدير او المحرر المسؤول الذي لا يمنع النشر عندما لا تتوفر الموانع الناتجة عن القوة القاهرة او الحادث الطارئ او الاكراه المادي أو المعنوي الذي لا يمكن دفعه اذا كون الفعل جناية او جنحة تتوفر فيها النية الإجرامية وتطبق العقوبة المقررة للجريمة المرتكبة مع خصمها الى حد النصف واذا كون الفعل جريمة خطيئة او مخالفة فتطبق العقوبة المقرر لها) ونصت المادة 31 من قانون المطبوعات الليبي رقم 76 الصادر سنة 1972 على المسئولية المتتابعة بالنسبة للجرائم المرتكبة بواسطة المطبوعات غير الدورية او شبة الدورية.

أصلـين إذا سـاهموا عمـداً فى ارتـكاب الجنـح المنصـوص عليهـا فى المـادة السـابقة متـى وقعـت بطريقـة الصحافـة[1].

والسـؤال المطـروح في هـذا الصـدد هـو عـن نـوع المسئولية الجنائيـة لوسـطاء تقديـم خدمـات شـبكة الانترنـت فـإذا كانـت شـبكة الانترنـت وسـيلة مـن وسـائل النـشر والعلانيـة مـما لا تثـور معـه صعوبـة في امكانيـة تطبيـق الاحـكام القانونيـة لجرائـم السـب والتشـهير، فـإن الجـدل القانـوني يثـور بالنسـبة لتحديـد المسـؤولين جنائيـا عـن السـلوك المرتكـب في الفضـاء الإليكـتروني وحـصر المسـاهمين فيـه، فمـن هـم الاشـخاص القائمـين عـلى تشـغيل الشـبكة و خدماتهـا المتعـددة؟ وبخاصـة أن المـشرع المـصري والعـربي نـص فقـط عـلي النـشر بواسـطة الصحـف.

اصبحـت الشـبكة العالميـة اليـوم تضـم مجموعـة مـن الانشـطة و الخدمـات المختلفـة فهـي بنيـة تحتيـة للاتصـالات اهـم خدماتهـا البريـد الالكـتروني e-MAIL و المنتديـات NEWS GROUP والناقـل TRANSFORSE PROTOCOL FTB لنقـل الملفـات بـين ارجـاء الشـبكة ووسـيلة المتصـل TELNET و هـو البرنامـج الـذي يتيـح لأي شـخص اسـتخدام برامـج ومميـزات حاسـوبية موجـودة في جهـاز اخـر بعيـد و لا توجـد في جهـاز المسـتخدم، امـا شـبكة المعلومـات WWW فهـي احـدى خدمـات الشـبكة مـن صفحـات مصححـة بلغـة HTML التـي تتيـح امكانيـة ربـط الصفحـات بالوسـائط (LINKS) وهـو سر تسـميتها بالشـبكة العنكبوتيـة[2].

فالسـؤال المطـروح هنـا هـو مـن هـم هـؤلاء الوسـطاء مـا الـدور الـذي يلعبـه كل وسـيط مـن علاقتـه بالمضمـون المنشـور عـلى الشـبكة.

---

(1) د. عادل ريان محمد. (1995م)، جرائم الحاسب الآلي وأمن البيانات، العربي، (440)، 73 – 77.

(2) فهد بن عبد الله اللحيدان، – الإنترنت، شبكة المعلومات العالمية - الطبعة الأولى- الناشر غير معروف - 1996. ص51 وما بعدها.

وسنعرض لذلك من خلال الآتي:

المطلب الأول: مقدمي الخدمة (I.S.P)INTERNET SERVICE PROVIDER)

المطلب الثاني: المسئولية الجنائية لمتعهد الايواء او المستضيف: (THE HOSTER)

المطلب الأول

مقدمي الخدمة

(I.S.P)INTERNET SERVICE PROVIDER

هو كل شخص يمد المستخدمين بالقدرة على الاتصال بواسطة انظمة حاسب الالي او يقوم بمعالجة البيانات و تخزينها بالنيابة عن هؤلاء المستخدمين: وهو ما نصت عليه المادة (1) (2) من اتفاقية بوداست 2001 بشان جرائم الانترنت، فمزود الخدمة هو من يمكن المشتركين من الوصول الى شبكة الانترنت عن طريق مدهم بالوسائل الفنية اللازمة للوصول الى الشبكة بمقتضى عقد توصيل الخدمة، فهو لا يقوم بتوريد المعلومة اوتأليفها[1]، و لا يملك أي وسائل فنية لمراجعة مضمونها، لأن دوره فني يتمثل في نقل المعلومات على شكل حزم الكترونية عن طريق حاسباته الخادمة، فهل يجوز اعتباره أحد المسؤولين عن الجريمة المعلوماتية ؟هنا ظهر اتجاهان نعرض لهما تباعاً:

اولا: الاتجاه القائل بعدم مسئولية المزود أو الوسيط أو الخادم:

و قد استند هذا الاتجاه الى أن مزود الخدمة لا يملك القدرة على التحكم في أي مضمون يبث على الشبكة، والقول بتقرير مسئوليته هنا يماثل القول بمسائلة مدير مكتب البريد و الهواتف على مدى مشروعية الخطابات والمكالمات التي تجري عبر هذه الخطوط[2] بل ان المسألة قد تنتهي بنا الى تقرير

(1) د. محمد فتحي عيد.(1419هـ). الإجرام المعاصر. الرياض: أكاديمية نايف العربية للعلوم الأمنية.ص12

(2) د.جميل عبد الباقي الصغير – الانترنت و القانون الجنائي - دار النهضة العربية 1992– ص119

مسـئولية الجهـات العامـة عـلى توفـير محطـات التقويـة لبـث القنـوات الفضائيـة المرئيـة، فتقريـر مسـؤولية مـزود الخدمـة يتطلـب أن يكـون دوره أكـثر إيجابيـة في بـث المـادة المجرمـة بالاضافـة الى أنـه لا يملـك الوسـائل الفنيـة التـي تمكنـه مـن مراقبـة تلـك المعلومـات المتدفقـة باعـداد تتجـاوز الملايـين[1].

ثانيا: الاتجاه القائل بتقرير مسؤولية مزود الخدمة:

انقسـم أنصار هـذا الاتجاه الى فريقين:

الاول: ينـادي بتقريـر المسـئولية الجنائية طبقا لاحكام المسـئولية المفترضة.

والثـاني: يذهـب الى تقريـر المسـئولية طبقـا للاحـكام العامـة للمسـئولية الجنائيـة [2].

مسـائلة مـزود الخدمة طبقا لأحكام المسـئولية المفترضة:

يبـدو لأول وهلـة اسـتجابة الـدور الـذي يقـوم بـه مـزود الخدمـة لهـذا النظـام اسـتنادا الى مسـاهمته في عمليـة النـشر و تحقيـق العلانيـة ووضعهـا في متنـاول المسـتخدمين.

الا ان المسـئولية المتتابعـة في مجـال النـشر بالنسـبة للمؤلـف والنـاشر تقـوم عـلى اسـاس العلـم المسبق بمـا تـم اعلانـه و نـشره للاخريـن، و هـو مـا يوجـب التـزام النـاشر او رئيـس التحـرر بالمراقبـة مـما لا يتوفـر بالنسـبة لمـزود الخدمـة، خاصـة عنـد قيامـه بالربـط اثنـاء المنتديـات المختلفـة حيـث يقـوم بتثبيـت تلـك المؤتمـرات

---

(1) د. مدحت رمضان – جرائم الاعتداء على الاشخاص و الانترنت – دار النهضة العربية – القاهرة – 2000 – ص 57-69.د. محمد عبد الطاهر حسين – المسئولية القانونية في مجال شبكات الانترنت - 2002 – دار النهضة العربية – القاهرة – ص 38

(2) د. هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001)، الطبعة الأولى، دار النهضة العربية ـ القاهرة، 2006، ص160 ؛ د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية،2002 ص13.

على جهازه الخادم و كل ما يصل لمزود الخدمة في هذه الحالات هي حزم من البيانات المشفرة[1].

و هو ما نصل معه الى عدم قبول تطبيق احكام المسئولية المتابعة لان مزود الخدمة لا يملك الوسائل الفنية و القانونية التي تمكن من مراقبة المضمون الذي ينشر و يتحرك على الشبكة.

مسائلة المزود طبقا للاحكام العامة للمسئولية الجنائية:

يستند اصحاب هذا الرأي الى أن مزود الخدمة لا يملك الوسائل الفنية اللازمة لمراقبة الصورة او الكتابة الا انه يملك الوسائل الفنية اللازمة لمنع الدخول الى هذه المواقع مما يؤدي الى تقديم المساعدة لاصحاب تلك المواقع عن طريق مدهم بالزائرين و هو ما تتحقق به المساهمة الجنائية التبعية بالمساعدة [2].

(1) V. dr. Mohammed Buzubar:"la Criminalite informatique sur L'internet"، Journal of law، (KwaitUniversity)، No.1، Vol.26، March 2002، P. 21 et s.

د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول: الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية ـ القاهرة، 1992، ص4 ـ 5 ؛ د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية ـ القاهرة، 1998، ص3؛ عبد الله العلوي البلغيثي:"الإجرام المعاصر ـ أسبابه وأساليب مواجهته»، ورقة مقدمة ضمن أشغال المناظرة الوطنية حول (السياسة الجنائية بالمغرب: واقع وآفاق)، التي نظمتها وزارة العدل بمكناس خلال الفترة من 9 ـ 11 دجنبر (ديسمبر) 2004، المجلد الأول، (الأعمال التحضيرية)، الطبعة الثانية، منشورات جمعية نشر المعلومة القانونية والقضائية، سلسلة الندوات والأيام الدراسية، العدد (3)، 2004، ص222.

(2) د. ذياب البداينة، المنظور الاقتصادي والتقني والجريمة المنظمة، ضمن أبحاث حلقة علمية حول الجريمة المنظمة وأساليب مكافحتها، التي نظمتها أكاديمية نايف العربية للعلوم الأمنية، 14 ـ 18 نوفمبر 1998، مركز الدراسات والبحوث ـ الرياض، 1999، ص209 وما بعدها ؛ كذلك انظر بالخصوص بحثنا السابق، ص81 ؛ بحثنا الموسوم بـ(الإرهاب والإنترنت)، مقدم إلى المؤتمر الدولي لجامعة الحسين بن طلال بعنوان: الإرهاب في العصر الرقمي، المنعقد بمدينة معان ـ الأردن، خلال الفترة 10 ـ 2008/7/13، ص1 وما يليها ؛ د. جميل الصغير، المرجع السابق، ص5 وما بعدها ؛ لواء دكتور/حسنين المحمودي بوادي، إرهاب =

لكـن يعـد هـذا الـراي أيضـا محـل نظـر، لان المسـاهمة الجنائيـة طبقـاً لاحـكام القانـون الجنـائي المـصري لا تكـون الا بالاعـمال السـابقة او المعـاصرة للسـلوك الاجرامـي و لا تكـون بالاعـمال اللاحقـة[1]، امـا مـزود الخدمـة فـدوره يـاتي لاحقـا لارتـكاب الجريمـة التـي تحققـت بكامـل عناصرهـا عـلى الشـبكة قبـل ان يبـدا دور مـزود الخدمـة[2].

هكـذا نصـل الى صعوبـة تطبيـق فكـرة العلـم المسـبق لاسـباب فنيـة وقانونيـة، فالاسـباب الفنيـة تتمثـل في عـدم وجـود الامكانيـة لمراقبـة المضمـون المنشـور قبـل نـشره امـا الاسـباب القانونيـة فترجـع الى عـدم اختصـاص مـزود الخدمـة بممارسـة اي نـوع مـن انـواع الرقابـة التوجيهيـة عـلى مـا يتـم نـشره لمـا في ذلـك مـن تعـارض و العديـد مـن الضمانـات الخاصـة بحـق المؤلـف و حـق الحيـاة الخاصـة، و لا يمكـن قبـول قيامهـا بـاي دور وقـائي عـلى الآخريـن[3].

إلا أننـا نـري انـه في حالـة إنـكار المسؤولية عـن مـزودي الخدمـة، والتـي تمثـل

= الإنترنت ـ الخطر القادم، الطبعة الأولى، دار الفكر العربي ـ الإسكندرية، 2006، ص49 وما بعدها ؛ محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية ـ الإسكندرية، 2004، ص7.

(1) د. جميل عبد الباقي الصغير – الانترنت و القانون الجنائي – دار النهضة العربية 2001- – ص 129 د.ا حمد السيد عفيفي – الاحكام اعامة للعلانية في قانون العقوبات – دراسة مقارنة - دار النهضة العربية – القاهرة - 2001 – 2002ص 551 - 552

(2) د. جميل عبد الباقي الصغير – الانترنت و القانون الجنائي – مرجع سابق– ص 132-134.

(3) ينص الفصل 575 من القانون الجنائي المغربي (من طبع في المملكة كلا أو بعضا من الكتب أو التصانيف الموسيقية أو الرسوم أو الصور الفنية أو أي إنتاج أخر مطبوع أو منقوش، مخالف بدلك القوانين والنظم المتعلقة بملكية مؤلفيها،يعد مرتكبا لجريمة التقليد، ويعاقب بغرامة من مائتين إلى عشرة آلاف درهم، سواء نشرت هده المؤلفات في المغرب أو في الخارج. ويعاقب بنفس العقوبة من يعرض هده المؤلفات المقلدة للبيع أو يوزعها أو يصدرها أو يستوردها) انظر في هذا المعنى بصدد جريمة السرقة، الدكتور محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، دار النهضة العربية، بيروت 1969 ص 63-64، الدكتور عبد الفتاح الصيفي: قانون العقوبات اللبناني جرائم الاعتداء على أمن الدولة وعلى الأموال دار النهضة العربية، بيروت 1972 ص 256.

البيئـة لإسـتقطاب المتطفلـين أو مـن يسـعون لـلإضرار بالآخريـن مـن إسـتخدام هـذه البيئـة، وبمـا يشـكل خطـرا عـلي المجتمـع بصفـة عامـة، ومـن سـيتم التعـرض لـه، بصفـة خاصـة، وبـأي وسـيلة، وأيـا كان حجـم الـضرر الـذي سـيتعرض لـه.

المطلب الثاني

المسئولية الجنائية لمتعهد الايواء او المستضيف

(THE HOSTER)

هو من يتولى ايواء صفحات معنية من الشبكة (WEB) على حساباته الخادمة (SERVER) مقابل أجر معين على الشبكة، حيث يقوم العميل و هو بمثابة المستاجر لتلك المساحة بكتابة المضمون الخاص عليها بطريقة مباشرة فيقوم بتخزين المادة المنشورة[1] و المادة المعلوماتية لكي يتمكن العميل من الوصول اليها في اي وقت [2].

كما يتولى مهمة تخزين وادارة المحتوى الذي قدمه له العميل فهو يساهم في عملية النشر دون أن يكون بامكانه السيطرة على المعلومة أو المضمون المنشور قبل عرضه على الانترنت، فهو يساعد المستخدم في الوصول الى الموقع و التجول فيه.

وهنا يثور التساؤل حول مدى تقرير المسئولية الجنائية بالنسبة له.

اولا: القول بعدم مسئولية مقدم الخدمة:

يطلب عاملو الايواء اعفاءهم من المسئولية الجنائية استنادا الى انهم يقومون بدور فني يتمثل في ايواء المعلومة و تخزينها لتمكين الجمهور من الاطلاع عليها و هو ما اخذ به المشرع الفرنسي في القانون رقم 719 الصادر سنة 2000 بتعديل قانون حرية الاتصالات، فنص التعديل على انتفاء المسئولية الجنائية و المدنية بالنسبة لكل الاشخاص الطبيعين او المعنويين الذين يتعهدون بالتخزين المباشر أو المستمر من اجل أن يضعوا تحت تصرف

---

(1) د. احمد السيد عفيفي – المرجع السابق – ص 554

(2) محمد حسن منصور – المسئولية الالكترونية – دار الجامعة – للنشر – الاسكندرية – 2003 – ص 202

الجمهور اشارات أو كتابات او صور او أغان أو رسائل، و لم يلزمهم هذا القانون الا بضرورة التحقق من شخصية المساهم في وضع المضمون أو كتابته و يستند أنصار هذا الاتجاه الى أن دور التخزين الذي يقوم به عامل الايواء لا يسمح بالسيطرة على المضمون[1].

ثانيا: القول بمسائلة عامل الايواء:

واجه الرأي السابق نقداً شديداً و ذهب راي آخر الى أن عامل الايواء يجب أن يكون مسئولا[2]، لان بامكانه رفض عملية الايواء (مقدم الخدمة) اذا شعر بعدم مشروعية المضمون المنشور[3].

ثالثاً: المسائلة طبقا للاحكام العامة المساهمة الجنائية:

اذا كان عامل الايواء يقوم باستضافة المعلومة او المضمون المنشور على صفحاته دون أن يكون لديه أي سيطرة على المضمون، فسلطته على هذا الاخير وعلمه به يشبه مدى علم المؤجر بالجرائم التي يرتكبها المستاجر في العين المؤجرة و في هذه الحالة تنتفي المسئولية الجنائية لعامل الايواء بمجرد ثبوت عدم علم عامل الايواء بالمضمون غير المشروع، خاصة وأن البيانات و المعلومات تتدفق بين أرجاء الشبكة بسرعة كبيرة[4]، و هو ما يتضح بصورة واضحة في المنتديات و مجموعات المناقشة [5].

---

(1) د. جميل عبد الباقي الصغير – المرجع السابق – ص 137-138

(2) المادة الأولى من القانون المغربي رقم-00 2بشأن حماية حق المؤلف والحقوق المجاورة. ويقصد بمصطلح برنامج الحاسوب وفق المادة الأولى من القانون المغربي المتعلق بحقوق المؤلف والحقوق المجاورة(كل مجموعة من التعليمات المعبر عنها بكلمات أو برموز أو برسوم أو بأي طريقة أخرى تمكن - حينما تدمج في دعامة قابلة لفك رموزها بواسطة آلة - أن تنجز أو تحقق مهمة محددة، أو تحصل على نتيجة بواسطة حاسوب أو بأي طريقة إلكترونية قادرة على معالجة المعلومات.)المادة 64-1

(3) د. جميل الصغبير– المرجع السابق – ص 135

(4) د. هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات،مكتبة الآلات الحديثة،أسيوط،1992،ص5.

(5) د.عمر محمد بن يونس، الجرائم الناشئة عن استخدام الإنترنت، الطبعة الأولى، دار =

أمـا بالنسـبة لباقـي الجرائـم المرتكبـة عـبر صفحـات (WEB) فانهـا مـن الجرائـم المسـتمرة الى يسـتمر اراتكابهـا باسـتمرار عرضهـا عـلى الصفحـة مـا يعنـي امكانيـة نشـوء قرينـة عـلى العلـم لهـا [1]، وهنـا يكـون عـلى المـشرع المـصري عنـد صياغـة الاحـكام العامـة للمسـئولية الجنائيـة للمسـتضيف أن يقـوم باعـمال الموازنـة بـين التزامـات هـذا الاخـير بعـدم عـرض المعلومـات غـير المشروعـة مـن جهـة حقـوق المؤلـف بالنسـبة لصاحـب المعلومـة مـن جهـة اخـرى.

رابعاً: مسائلة عامل الايواء طبقا لاحكام المسئولية المفترضة(المتتابعة)[2]:

نخلـص مـن كل مـا تقـدم الى: صعوبـة تطبيـق الأحـكام العـام عـلى أي مـن الوسـيطين لصعوبـة اثبـات العلـم بالمضمـون المجـرم مـما تنتفـي معـه الوحـدة المعنويـة بـين المسـاهمين أمـا احـكام المسـئولية المتتابعـة فـلا يمكـن تطبيقهـا ايضـا لا لصعوبـة مراقبـة المضمـون فحسـب بـل لاعتبـار اخـر لا يقـل اهميـة و هـو أن احـكام المسـئولية المفترضـة (المتتابعـة) اسـتثناء مـن الأصـل العـام لا يجـوز التوسـع فيـه.

فالمسـئولية الجنائيـة يجـب ان تتقـرر بنـص صريـح و يجـب ان ترتبـط بامكانيـة السـيطرة عـلى المعلومـة فالوسـيط في تقديـم هـذه الخدمـات سـواءً كان مـزود الخدمـة او عامـل الايـواء، عبـارة عـن وسـيط تجـاري يقـوم باعـمال الوسـائط في CYBER SPACE و هـو مـا يميـزه عـن الوسـيط التقليـدي الـذي يكـون قريبـا مـن الاطـراف و اكـثر قـدرة عـلى تقييـم تصرفاتهـم بينـما الوسـيط المعلومـاتي يقـوم

=النهضـة العربيـة ـ القاهـرة، 2004، ص785 ومـا بعدهـا ؛ د.هشـام محمـد فريـد رسـتم، الجوانـب الإجرائيـة للجرائـم المعلوماتيـة ـ دراسـة مقارنـة، مكتبـة الآلات الحديثـة ـ أسـيوط، 1994، ص5 ومـا يليهـا؛ نبيلـة هبـة هـروال، الجوانـب الإجرائيـة لجرائـم الإنترنـت في مرحلـة جمـع الاسـتدلالات ـ دراسـة مقارنـة، (رسـالة ماجسـتير)، دار الفكـر الجامعـي ـ الإسـكندرية، ص35 ومـا بعدهـا.

(1) د. جميل الصغير، مرجع سبق ذكره، ص142

(2) ان القانون رقم 73 لسنة 1972 بشان المطبوعات الليبي ينص في المادة 31 على أن المطبوعات تشمل الكتابات و الصور و الرسوم، و لما كان ما يبث على الشبكة يعد من الكتابات، فان اعتبار عامل الايواء هنا قائما بدور رئيس التحرير تواجهه عقبة فنية تتمثل في عدم قدرته على مراقبة المضمون

بـدور الوسـيط في بيئـة افتراضيـة تنعـدم فيهـا الحـدود الجغرافيـة اللازمـة للاقـتراب والتقييـم كـما تنعـدم فيهـا النظـم القانونيـة الحاكمـة مـن جهـة اخـرى [1].

وهـو مـا نصـل معـه الى ضرورة التعـرض إلى البعـد الـدولي للجريمـة المعلوماتيـة و الطبيعـة اللامركزيـة للنطـاق الـذي ترتكـب فيـه هـذه الجريمـة حيـث تنعـدم حـدود الزمـان و المـكان الـذي ترتكـز عليـه اسـس القواعـد الإجرائيـة التقليديـة، فـما هـي التحديـات الإجرائيـة للجرائـم المعلوماتيـة و كيـف يمكـن مواجهتهـا؟[2]

(1) Chriss Reed،Internet Law- 2004 - CAMPRIDGE UNIVERCITY PRESS، p.89

(2) انظر: أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والإنترنت ـ دراسة تحليلية مقارنة، الطبعة الأولى، دار وائل للنشر ـ عمان ـ الأردن، 2000، ص105 ؛ بحثنا السابق"السياسة الجنائية في مواجهة جرائم الإنترنت Cyber Crimes»، ص90.

المبحث الثاني

الآلية الإجرائية للجريمة المعلوماتية

من المعلوم أن الجريمة المعلوماتية ترتكب باستخدام التقنية المعلوماتية مما يعني أنها ترتكب في فضاء افتراضي مفرغ cyberspace، سواء ارتكبت عبر شبكة الإنترنت أم في داخل نطاق ذات المؤسسة التي يتم الاعتداء عليها، أو ارتكاب الجريمة من خلالها، فضلا عن المشكلات الموضوعية التي تثيرها هذه الجرائم في تطبيق القواعد التقليدية لقانون العقوبات الذي صيغت جل نصوصه ونظمه الأساسية لتواجه سلوكاً مادياً يرتكب في عالم مادي ملموس، فإذا كان ذلك هو حال القواعد الموضوعية للتجريم و العقاب، فما هو حال القواعد الإجرائية لهذا الفرع من القانون الجنائي ؟

وهو ذلك الفرع الذي يتأسس في كل النظم القانونية المختلفة على مبدأ دستوري هو الشرعية، أي شرعية التجريم و العقاب، الذي تنبثق عنها قاعدة الشرعية الإجرائية[1].

و ما يميز هذه الجريمة هو أنها ترتكب، في نطاق رقمي يختلف كلياً عن النطاق التقليدي الذي ترتكب فيه الجريمة حيث يتم الاستدلال عليها وضبطها و اثباتها بالوسائل التقليدية المتمثلة في اجراءات الاستدلال والتحقيق، فهي اجراءات صيغت لضبط واثبات جرائم ترتكب في عالم ملموس مادياً، يلعب فيه السلوك المادي الدور الأكبر و الأهم، وهنا يثور التساؤل حول مدى صلاحية هذه الإجراءات لضبط وإثبات جريمة ارتكبت في عالم افتراضي غير ملموس ؟

---

(1) د. هشام رستم، ص18 ؛ أسامة المناعسة وآخرون، ص289 ؛ د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية ـ القاهرة، 2002، ص113 وما بعدها.

أما إذا ارتكبت الجريمة عبر الشبكة العنكبوتية الدولية [1](الانترنت) تزداد العقبات القانونية صعوبة، فلا نكون أمام مشكلات اجرائية تخص ضبط الجريمة و اثباتها فحسب، بل نجد انفسنا أمام مشكلة أكثر تعقيداً تتمثل في تحديد الاختصاص القضائي المرتبط بتحديد القانون الواجب التطبيق على هذه الجريمة، فقواعد الاختصاص القضائي التقليدية صيغت لكي تحدد الاختصاص المتعلق بجرائم قابلة للتحديد المكاني للجريمة، وهي قواعد ترتكز على مبدأ الإقليمية، وهو ما يرتبط بسيادة الدولة على إقليمها[2].

فلا يكون الخروج عليه بقبول اختصاص قضائي أجنبي إلا في حالات استثنائية يجب النص عليها صراحة، وهنا تثور امامنا مدى امكانية الاعتماد على هذه القواعد لتحديد الاختصاص القضائي لجريمة ترتكب في مجال تنعدم فيه الحدود الجغرافية، وكثيرا ما يكون مرتكبيها في بلاد مختلفة و من جنسيات متعددة، و كثيرا ايضا ما يتعلق السلوك الاجرامي باكثر من دولة: الدولة التي ارتكب فيها السلوك و الدولة التي تم فيها القبض على الجاني و تلك التي حدثت فيها النتيجة الاجرامية و هو ما يتطلب منا التطرق الى مشكلات ضبط الجريمة المعلوماتية و اثباتها، ثم عن مشكلات الاختصاص بنظر الجريمة المعلوماتية، والأهم من ذلك تحديد المكان في حالة الجرائم المستمرة.

وسنعرض لذلك من خلال الآتي:

المطلب الأول: ضبط الجريمة المعلوماتية.

المطلب الثاني: قواعد الاختصاص.

---

(1) . عطية عثمان محمد بوحويش، حجية الدليل الرقمي في إثبات جرائم المعلوماتية، رسالة التخصص العالي (الماجستير)، مقدمة إلى أكاديمية الدراسات العليا/فرع بنغازي، للعام الجامعي 2009، ص70.

(2) د. جميل الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، ص115 ؛ عطية بوحويش، ص73 وما بعدها.

المطلب الأول

ضبط الجريمة المعلوماتية

يعتمد ضبط الجريمة و اثباتها في المقام الأول على جمع الادلة التي حدد المشرع وسائل اثباتها على سبيل الحصر، وذلك لما فيها من مساس بحرية الأفراد وحقوقهم الأساسية، فلا يجوز أن تخرج الأدلة التي يتم تجميعها عن تلك التي اعترف لها المشرع بالقيمة القانونية، و تتمثل في وسائل الاثبات الرئيسية و في المعاينة و الخبرة و التفتيش و ضبط الأشياء المتعلقة بالجريمة، أما غيرها من وسائل الاثبات كالاستجواب و المواجهة و سماع الشهود فهي مرحلة تالية من إجراءات التحقيق و جمع الأدلة، ولما كنا بصدد تناول الجريمة المعلوماتية و ما تثيره من مشكلات إجرائية[1].

فسنتعرض للمشكلات القانونية التي يثيرها اثبات هذه الجرائم دون غيرها من الاجراءات كالاستجواب و المواجهة و سماع الشهود، لأن هذه الأخيرة تتم في مواجهة البشر، أما المعاينة و الخبرة و التفتيش، فهي إجراءات فنية محلها الأشياء لا الافراد وهو ما يهمنا في هذا الموضوع.

وسنعرض لذلك في الفروع الآتية:

الفرع الأول: حجية المخرجات الاليكترونية في الاثبات.

الفرع الثاني: الخبرة و المعاينة في الجرائم المعلوماتية.

---

(1) أسامة المناعسة وآخرون، ص280 وما بعدها ؛ د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ـ دراسة مقارنة، الطبعة الأولى، دار النهضة العربية ـ القاهرة، 1997، ص77 وبما بعدها.

الفرع الأول

حجية المخرجات الاليكترونية في الاثبات

تخضع المحررات كغيرها من الأدلة التي تقدم أثناء نظر الدعوى إلى تقدير المحكمة حيث يسود مبدأ حرية القاضي في تكوين عقيدته، وهو ما يختلف فيه القاضي المدني حيث يتقيد هذا الاخير بطرق معينة في الاثبات، فالقاضي الجنائي له مطلق الحرية في تقدير الدليل المطروح أمامه، وله أن يأخذ به أو يطرحه ولا يجوز تقييده بأي قرائن أو افتراضات[1].

ولما كانت المحررات أحد الادلة التي قد يلجأ اليها القاضي في الاثبات فهي تخضع كغيرها من الادلة لتقدير المحكمة، الا إذا كان الاثبات متعلقاً بمواد غير جنائية، ففي هذه الحالة يكون على القاضي الجنائي أن يتقيد بطريق الاثبات المحددة في ذلك الفرع من القانون مثال ذلك حق الملكية في جريمة السرقة، والعقود التي تثبت التصرف في الحق في جريمة خيانة الامانة أو صفة التاجر في جريمة التفالس بالتدليس[2].

وهنا تثور مشكلة مدى حجية المخرجات الاليكترونية في الاثبات الجنائي في هذه الحالات، فللمخرجات الاليكترونية انواع مختلفة، فهي تتنوع بين مخرجات ورقية، و مخرجات لا ورقية و هي المعلومات المسجلة على الأوعية الممغنطة كالاشرطة و الاقراص المرنة Floppy Disk القرص الصلب Hard Disk وغيرها من الاوعية التي اصبحت في تطور مستمر حتى وصلت الى اقراص الflash discs التي اصبحت تتميز بسعات كبيرة للتخزين، خاصة أنه تواجهنا مشكلة اساسية تتعلق بصعوبة التمييز

---

(1) د. مأمون سلامة - الاجراءات الجنائية في التشريع الليبي – ج 2ط-2000 منشورات المكتبة الجامعة – ص151.

(2) د.مأمون سلامة – المرجع السابق – ص160

بين المحرر و صورته أو بين الاصل و الصورة، ذلك لأننا نتعامل مع بيئة اليكترونية تعمل بالنبضات، والذبذبات و الرموز و الأرقام وهو ما يستحيل معه تطبيق القواعد الخاصة بالمحررات العرفية [1]

ولما كان المشرع المصري لا يزال عازفاً عن التدخل التشريعي في هذه المسألة فلا نجد بداً من تطبيق القواعد العامة في هذا الصدد، ولما كان ذلك، فالمشرع المصري لا يزال يعتمد على مبدأ سيادة الدليل الكتابي على غيره من الادلة ولا يجوز الاعتماد على الدليل غير الكتابي في غير المسائل الجنائية، الا على سبيل الاستئناس، ولا يخفى ما يؤدي ذلك من تقييد للقاضي الجنائي لأن الإثبات في المسائل الجنائية كثيراً ما يعتمد على مسائل غير جنائية، وهو ما سبقت الاشارة اليه عند تناول جريمة التزوير في هذا البحث التي اعتمدت على مدى اعتبار هذه الاوعية من قبيل المستندات او المحررات موضوع جريمة التزوير، فمواجهة الجرائم المعلوماتية لا تتأتى الا عن طريق نظام قانوني متكامل أهم عناصره التدخل لضبط المعاملات و التجارة الاليكترونية وإضفاء الحجية القانونية على المستندات الاليكترونية شأنها شأن المستندات الورقية فيما يتعلق بالإثبات الجنائي، وأن تكون دلالاتها يقينية للقاضي الجنائي، حتى يتاح للقاضي الجنائي الاعتماد عليها [2]، كغيره من الادلة، وقد كان المشرع التونسي من السباقين بين أقرانه على المستوى العربي في هذا المجال، حيث صدر في تونس قانون التجارة و المعاملات الاليكترونية الذي اعترف للمستندات الاليكترونية سنة 2000 بحجيتها في الاثبات.

كما أصدرت امارة دبي قانون التجارة الاليكترونية سنة 2002، وتبعهما بعد ذلك المشرع المصري سنة 2004 الذي اصدر قانون نظم التوقيع

(1) د. احمد شرف الدين- حجية الرسائل الاليكترونية في الاثبات – شبكة المعلومات القانونية العربية East Law.com - 2007-

(2) د. عمر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي"المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية»، الطبعة الأولى، 2004 ـ 2005، ص201 ـ 204.

اليكـتروني، وتجـدر الاشـارة في هـذا الصـدد إلى القانـون العـربي النموذجـي السـابق الاشـارة اليـه سـنة 2003، وكل هـذه القوانـين اعطـت للمسـتند الاليكـتروني ذات الحجية التـي يتمتـع بهـا المحـرر الورقـي، تجـدر الاشـارة ايضـاً إلى أن لجنـة الأمـم المتحـدة للقانـون التجـاري الـدولي (United Nation Commission on International Trade Law UNCITRAL) عـلى هـذه الحجيـة و قـد كان ذلـك سـنة 2000.

أمـا القانـون العـربي النموذجـي فنـص في المـادة الأولى منـه عـلى تعريـف الكتابـة بأنهـا كل: (عمليـة تسـجيل للبيانـات عـلى وسـيط لتخزينهـا)، و المقصـود بالوسـيط في هـذه الحالـة هـو الوسـيط الاليكـتروني لأن الوسـيط الورقـي المتمثـل في الأوراق التقليديـة لا يحتـاج إلى تعريـف، وإن كنـا نتحفـظ عـلى اسـتخدام عبـارة الوسـيط دون تحديـده بالاليكـتروني، مـا دام الأمـر متعلقـاً بالتجريـم و العقـاب، أمـا المـادة 6 مـن قانـون الاونسـترال النموذجـي السـابق الاشـارة اليـه.

اذا كان المـشرع التونـسي يعـد سـباقاً إلى اللحـاق بهـذا التطـور التشريعـي فـإن المـشرع السـنغافوري أصـدر قانـون اللإثبـات أقـر فيـه حجيـة المسـتندات المعلوماتيـة في الاثبـات منـذ سـنة 1997م وهـو مـا يبـين مـدى تأخـر المـشرع المـصري في مواكبـة هـذا التطـور[1].

---

(1) د. علي أحمد راشد، المدخل وأصول النظرية العامة 1974، ص185 ؛ د. عدنان الخطيب، موجز القانون الجزائي، الكتاب الأول، المبادئ العامة في قانون العقوبات، مطبعة جامعة دمشق، 1963، ص79 ؛ د. موسى مسعود ارحومة، الأحكام العامة لقانون العقوبات الليبـي، الجزء الأول، النظرية العامة للجريمة، الطبعة الأولى، منشورات جامعة قاريونس (بنغازي)، 2009، ص110 وما يليها.

R. Vouin et J. Léauté، droit pénal et procédure pénale، 2 me éd.، Paris، 65، P. 19 ; MohieddineAmzazi، Présis de droit Criminel، 1 ère éd.،1994 4، Dar Nachr Al Maarifa، Rabat، P. 62

الفرع الثاني

الخبرة و المعاينة في الجرائم المعلوماتية

تعتبر كل من الخبرة و المعاينة أكبر العقبات التي تواجه الاثبات في الجرائم المعلوماتية، فالمعاينة اجراء بمقتضاه ينتقل المحقق الى مكان وقوع الجريمة ليشاهد اثارها بنفسه، فيقوم بجمعها وجمع أي شيء يفيد في كشف الحقيقة، وتقتضي المعاينة اثبات حالة الأشخاص و الأشياء الموجودة بمكان الجريمة و رفع الآثار المتعلقة بها كالبصمات و الدماء و غيرها مما يفيد التحقيق، و المعاينة تكون شخصية إذا تعلقت بشخص المجني عليه، أو مكانية اذا تعلقت بالمكان الذي تمت فيه الجريمة، ووضع الشهود و المتهم و المجني عليه، أما المعاينة العينية فهي التي تتعلق بالأشياء أو الأدوات المستخدمة في ارتكاب الجريمة وقد يقتضي الامر الاستعانة بخبير للتعرف على طبيعة المادة او نوعها إذا كان ذلك يحتاج لرأي المتخصص، وفي هذه الحالة يتم ارسال هذه الاشياء الى الخبير لنكون امام بصدد اجراء آخر من اجراءات التحقيق و هو الخبرة، فالخبرة هي أحد أهم وسائل جمع الأدلة، يلجأ اليها المحقق عند وجود واقعة مادية أو شيء مادي يحتاج التعرف عليه إلى حكم الخبير المتخصص، فهو يأخذ حكم الشاهد من حيث الحجية أو القوة في الاثبات، أوليس من الاجدر العمل علي إقرار المسؤولية الجنائية علي الوسيط المعلوماتي بما يتيح التوصل إلي الفاعل الحقيقي ويمكن العمل علي منح عفو من العقاب في حالة الإدلاء بمعلومات تفيد في الإدانة.

يثور التساؤل هنا عن مدى امكانية معاينة الجريمة المعلوماتية[1]، أما

---

(1) واذا كانت المادة 74 اجراءات جنائية ليبي تنص على انتقال المحقق لأي مكان ليثبت حالة الامكنة و الاشياء و الاشخاص ووجود الجريمة مادياً، فهل يكون للجريمة المعلوماتية وجود مادي، يمكن للمحقق الليبي معاينته؟ نجد في هذه المادة أن المشرع سن هذا النص لضبط جريمة لها وجود مادي محسوس في العالم الخارجي، وما يؤكد ذلك هو أن المادة 44 من ذات

السلوك الاجرامي في في الجريمة المعلوماتية فهو عبارة عن بيانات مخزنة في نظام معلوماتي يتطلب اثباته انتقال محقق متخصص حيث يتم التفتيش عن البيانات عن طريق نقل محتويات الاسطوانة الصلبة الخاصة بالجهاز، ويجب على المحقق أو ضباط الشرطة المتخصصين استخراج المعلومات التي من شأنها أن تساعد التحقيق وأن يطلعوا زملائهم عليها، مثل القيام بالبحث في بنوك المعلومات وفحص كل الوثائق المحفوظة ومراسلات مرتكب الجريمة مثل الرسائل الإلكترونية وفك شفرات الرسائل المشفرة، وهو ما يحدث عندما ترتكب الجريمة عبر شبكة الانترنت، ولكي ينجح المحققون في عملهم يجب أن يقتفوا أثر الاتصالات من الحاسب المصدر إلى الحاسب أو المعدات الأخرى التي تملكها الضحية، مروراً بمؤدي الخدمة والوساطة في كل دولة، وهو ما يتطلب وجود محققين يتمتعون بخبرة في هذا المجال، كما ان هناك ضرورة للتعاون الدولي، وأن تعمل الشرطة الدولية الإنتربول من إيجاد آلية للكشف عن هذه الجرائم.

كما يقتضي ذلك ايضاً ان يعمل المحقق على الوصول إلى الملفات التاريخية التي تبين لحظات مختلف الاتصالات، من أين صدرت؟ ومن الذي يحتمل إجراؤها، بالاضافة الى ضرورة إلمام المحقق بالحالات التي يكون عليه فيها التحفظ على الجهاز أو الاكتفاء بأخذ نسخة من الاسطوانة الصلبة للحاسب، والاوقات التي يستخدم فيها برامج استعادة المعلومات التي تم الغاؤها[1].

القانون تنص على أن (توضع الاشياء و الاوراق التي تضبط في حرز مغلق وتربط كلما أمكن) فالحرز المغلق الذي يتم ربطه هو الاجراء العام الذي تخضع له كل الاشياء المضبوطة،وهنا نصطدم بالعقبة الاساسية أمام معاينة الجريمة المعلوماتية التي ترتكب داخل الفضاء المعلوماتي أو السيبراني، فالمحقق في هذه الحالة يتعامل مع بيئة مليئة بالنبضات الاليكترو مغناطيسية و البيانات المخزنة داخل نظام معلوماتية شديدة الحساسية ولا يتعامل مع أوراق او اسلحة أو اشياء قابلة للربط وهو ما يؤكد القواعد الاجرائية التقليدية سنت لتواجه سلوكاً ماديا يرتكب بواسطة الات و ادوات قابلة للربط و التحريز.

(1) Recommandations sur le dépistage des communications électroniques transfrontalière dans le cadre des enquêtes sur les activités criminelles www G8 Mont tremblant Canada 21 mai 2002.

اشار اليه أ.د. صالح أحمد البربري دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية -الموقعة في بودابست في 2001-/11/3 www.arablawinfo.com

فالمحقق الذي يقوم بمعاينة الجريمة المعلوماتية يجب أن يكون ملماً بمهارات هذه التقنية، مثل القدرة على استخدام برامج Time stamp وهي البرامج التي يمكن عن طريقها تحديد الزمن الذي تم فيه السلوك الاجرامي، لأن ذلك لا يكون متاحاً في جميع الانظمة المعلوماتية، أما الخبير ففي هذه الحالة يجب ان يكون ملماً بمهارات تحليل البيانات و مهارات التشفير cryptanalysis skills التي تتيح له فك الرموز وإستعادة البيانات الملغية[1].

ولما كانت الجرائم ترتكب عبر الشبكة الدولية فقد نصت المادة 23 على أن (تتعاون كل الأطراف، وفقاً لنصوص هذا الفصل، على تطبيق الوسائل الدولية الملائمة بالنسبة للتعاون الدولي في المجال الجنائي والترتيبات التي تستند إلى تشريعات موحدة ومتبادلة وكذلك بالنسبة للقانون المحلي على أوسع نطاق ممكن بين بعضهم البعض بغرض التحقيقات والإجراءات المتعلقة بالجرائم الجنائية للشبكات والبيانات المعلوماتية وكذلك بشأن الحصول على الأدلة في الشكل الإلكتروني لمثل هذه الجرائم).

كما نصت المادة 30 من الاتفاقية على الكشف السريع عن البيانات المحفوظة حيث نصت على: أنه عند تنفيذ طلب حفظ البيانات المتعلقة بالتجارة غير المشروعة والمتعلقة باتصال خاص تطبيقاً لما هو وارد في المادة 29 فإن الطرف المساند إذا اكتشف وجود مؤدي خدمة في بلد آخر قد شارك في نقل هذا الاتصال فإن عليه أن يكشف على وجه السرعة إلى الطرف طالب المساعدة كمية كافية من البيانات المتعلقة بالتجارة غير المشروعة[2] حتى

(1) P. WILHEM،"La hiérarchie des responsabilité sur Internet"، précité، p. 4.

(2) د. موسى مسعود ارحومة، تحديد النطاق المكاني لجرائم تلويث البيئة البحرية والقانون الواجب التطبيق، ورقة مقدمة إلى المؤتمر العلمي الخامس لكلية الشريعة والقانون/جامعة إربد الأهلية بعنوان:"البيئة في ضوء الشريعة والقانون ـ واقع وتطلعات" الأردن، خلال الفترة 12 ـ 13/تموز (يوليو) 2006، ص5 وما بعدها.

يمكن تحديد هوية مؤدي الخدمة هذا والطريق الذي تم الاتصال من خلاله، كما أشارت المادة 31 إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة، حيث أجازت لأي طرف أن يطلب من أي طرف آخر أن يقوم بالتفتيش أو أن يدخل بأي طريقة مشابهة وأن يضبط أو يحصل بطريقة مماثلة، وأن يكشف عن البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكاني لذلك الطرف والتي يدخل فيها أيضاً البيانات المحفوظة وفقاً للمادة 29من الاتفاقية.

وهو ما نصل معه الى حقيقة مؤداها اننا نواجه اليوم اخطر مظاهر العولمة، فالتعاون الدولي في المجال الجنائي لم يعد مقتصراً على نظام الانتربول، فأصبح على الدولة أن تستخدم بروتوكولات موحدة لنظم التخزين و الحماية المعلوماتية كما حدث على مستوى الاتصالات الهاتفية، لأن التعاون بين دولة واخرى سوف يتم بين أجهزة الخبرة الجنائية بشكل مباشر وبطريقة متشابكة، وهو ما نصل معه إلى ان تطوير البنية التحتية المعلوماتية لأي دولة اليوم اصبح ضرورة ملحة، ومطلباً أساسياً قد يترتب على غيابه انعزال الدولة وصيرورة نظامها المعلوماتي - اذا كان متواضعاً - مباحاً لمجرمي المعلوماتية [1].

نخلص من كل ما تقدم إلى أن: الخبرة و المعاينة الجنائية في الجرائم المعلوماتية اليوم تحتاج إلى ادارة خاصة يعمل بها متخصصون في أنظمة المعلومات ويتمتعون بصفة الضبطية القضائية، وهو ما يتطلب انشاء ادارة خاصة للخبرة و المعاينة في الجرائم المعلوماتية، ولا يجب الاكتفاء بمجرد تدريب القائمين على إدارة الخبرة الجنائية، أما رجال القضاء و النيابة

---

(1) ممدوح خليل عمر – حماية الحياة الخاصة والقانون الجنائي – دار النهضة العربية القاهرة 1983 ص 207.أسامة عبد الله قايد – الحماية الجنائية للحياة الخاصة وبنوك المعلومات – دار النهضة العربية القاهرة 1994 ص 48

والضبطيـة القضائيـة فـلا شـك أنهـم يحتاجـون للتدريـب عـلى اسـتخدام مهـارات الحاسـب الآلي و و الموسـوعات القانونيـة التـي تتطلـب ربـط كافـة المؤسسـات القضائيـة بقواعـد بيانـات قانونيـة مثـل أحـكام المحاكـم و القوانـين المختلفـة، لتوفـير امكانيـة اسـتخدام موسـوعات القوانـين و مجموعـات الأحـكام القانونيـة العربيـة المختلفـة و تعليـمات النائـب العـام، لرفـع مسـتوى الكفـاءة القانونيـة لـدى رجـال القضـاء و النيابـة العامـة [1].

(1) أ.د. صالح أحمد البربري - دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية - الموقعة في بودابست في 23/11/2001-www.arablawinfo.com - ص2

المطلب الثاني

قواعد الاختصاص

خلصنا إلى عدم كفاية القواعد التقليدية للخبرة و المعاينة، وعدم ملاءمتها لاثبات الجرائم المعلوماتية، فهل تستجيب القواعد الخاصة بتحديد نطاق تطبيق القانون من حيث المكان، فكيف يمكن تحديد مكان وقوع الجريمة المعلوماتية ؟

واذا كانت هذه الجريمة ترتكب في مجال افتراضي غير محدد جغرافياً فهل يمكن ربط هذه الجريمة بدولة ما دون اخرى، فإن ذلك يتطلب ضرورة الحديث عن لا مركزية الفضاء المعلوماتي، قبل تناول التعاون الدولي لملاحقة الجريمة المعلوماتية[1]، وهل سيقتصر العلم بالجريمة، بما يتم الإبلاغ عنه، وبخاصة في حالة ان معرفة حجم الضرر أمر يعتمد علي مدي خبرة المضرور نتيجة العمل غير المشروع من جانب المجرم المعلوماتي، والتي تعتمد في أفعالها علي المنتديات، أو علي المواقع التي تقدم خدمات، بمعني أدق من خلال مقدمي خدمات المعلوماتية أو وسطاء الخدمة.

وسنتناول ذلك في الفرعين التاليين:

الفرع الأول: عالمية الجريمة المعلوماتية.

الفرع الثاني: النطاق المكاني.

---

(1) د. كمال أنور محمد القاضي، تطبيق قانون العقوبات من حيث المكان، رسالة دكتوراه، مقدمة إلى كلية الحقوق ـ جامعة القاهرة، 22 إبريل 1965، دار مطابع الشعب، ص90 وما يليها

الفرع الأول

عالمية الجريمة المعلوماتية

لم تعد للحدود الجغرافية أي اثر في الفضاء الشبكي او الآلي، فهو لا يعترف بالحدود الجغرافية حيث يتم تبادل البيانات في شكل حزم الكترونية توجه الى عنوان افتراضي ليس له صلة بالمكان الجغرافي، فهو فضاء ذو طبيعة لا مركزية DESSENTRALI ZED NATURE و يمكن اجمال اهم خصائصه في عدم التبعية لاي سلطة حاكمة [1].

فالفضاء الآلي: نظام الكتروني معقد لانه عبارة عن شبكة اتصال لا متناهية غير مجسدة و غير مرئية، ومتاحة لاي شخص حول العالم و غير تابعة لاي سلطة يمكن أن تحدد نطاقها أو مسلكها، فالفعل المرتكب فيها يتجاوز الاماكن بمعناه التقليدي وله وجود حقيقي وواقعي لكنه غير محدد المكان لكنه حقيقة واقعة.

فالشبكة عالمية النشاط و الخدمات لا تخضع لاي قوة مهيمنة الا في بدايتها حيث كان تمويل هذه الشبكة حكوميا يعتمد على المؤسسة العسكرية الامريكية، أما الآن فقد اصبح التمويل ياتي من القطاع الخاص حيث الشركات الاقليمية ذات الغرض التجاري التي تبحث عن كافة السبل للاستفادة من خدماتها بمقابل مالي [2].

---

(1) د. أحمد عبد الكريم سلامة، قانون حماية البيئة ـ دراسة تأصيلية في الأنظمة الوطنية والاتفاقية، الطبعة الأولى، منشورات جامعة الملك سعود ـ السعودية، 1418هـ (1997)، ص535.

(2) د. منير الجنبهي- ممدوح الجنبهي- صراخ الانترنت وسائل مكافحتها – المرجع السابق -ص 9.د. فتوح الشاذلي – القانون الدولي الجنائي – دار المطبوعات الجامعية – الاسكندرية – 2001 – ص 34

والجريمـة المرتكبـة عـبر شـبكة الانترنـت جريمـة تعـبر الحـدود و القـارات، و هـو مـا يدرجهـا ضمـن موضوعـات القانـون الجنـائي الـدولي.

و قـد ازدادت اهميـة القانـون الجنـائي الـدولي بعدمـا تطـورت الجريمـة المنظمـة في وقـت تقلـص فيـه المفهـوم التقليـدي للسـيادة، حيـث اتسـع نظـام المعاهـدات الدوليـة لمكافحـة الجرائـم العابـرة للحـدود فالجانـب الـدولي للجريمـة المعلوماتيـة لا يعـد عنـصرا مـن عناصرهـا كـما هـو الحـال في الجريمـة الدوليـة بـل يعـد هـو نطاقهـا المـكاني.

ان القواعـد العامـة التـي تحكـم نطـاق تطبيـق النصـوص الجنائيـة - التـي تتمثـل في مبـدأ اقليميـة النـص الجنـائي و الاسـتثناءات الـواردة عليـه - تقتـضي تطبيـق النـص الجنـائي عـلى كل الجرائـم الواقعـة في اقليمـه.

الفرع الثاني

النطاق المكاني

يعتمـد النظـام القانـوني عـلى جريمـة ترتكـب في مـكان قابـل للتحديـد الجغـرافي، اما الجريمـة المعلوماتيـة فهـي جريمـة ترتكـب في نطـاق غـير قابـل للتحديـد الجغـرافي، الا انـه يضـم اكـبر تجمـع إنسـاني يتميـز بارتبـاط و تشـابك معقـد، و تتمثـل اهـم خصائصـه في خلـق آليـات خاصـة لفـرض الالتزامـات و الاذعـان لهـا مثـل قطـع الاتصـال عـلى مخترقـي بعـض القواعـد او طردهـم مـن المنتديـات، لكـن هـذا التجمـع الانسـاني الضخـم يفتقـر الى المعايـير الاخلاقيـة المشـتركة[1].

و هـو مـا حـدا المجلـس الاوروبي الى عقـد اتفاقيـة بوداسـت COUNCIL السـابق الاشـارة اليهـا، و التـي قدمـت صـورا لمكافحـة هـذه الجرائـم و نصـت المـادة 22 منهـا عـلى"أن لـكل طـرف اتخـاذ الإجـراءات التشريعيـة وغيرهـا التـي يراهـا لازمـة لـكي يحـدد اختصاصـه بالنسـبة لـكل جريمـة تقـع وفقـاً لمـا هـو وارد في المـواد مـن 2 إلى 11 مـن الاتفاقيـة الحاليـة عندمـا تقـع الجريمـة[2]:

أ- داخل النطـاق المحلي للدولة.

ب- عـلى ظهر سـفينة تحمـل علم تلك الدولة.

ج- عـلى متن طائرة مسجلة في هذه الدولة.

د- بواسـطة أحـد رعاياهـا، إذا كانـت الجريمـة معاقبـاً عليهـا جنائيـاً في

---

(1) الدكتور. سالم محمد سليمان الأوجلي: أحكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، رسالة دكتوراه، كلية الحقوق جامعة عين شمس 1997م ص 425

(2) USA V. Thomas، no. cr – 94 – 20019 – 9 (w. d. tenn.1994).

مشار إليها عند: د. عمر محمد بن يونس، الجرائم الناشئة عن استخدام الإنترنت، ص908.

المكان الذي ارتكبت فيه أو إذا كانت الجريمة لا تدخل في أي اختصاص مكاني لأي دولة أخرى.

ولكل طرف أن يحتفظ لنفسه بالحق في عدم تطبيق، أو عدم التطبيق إلا في حالات وفي ظل شروط خاصة، قواعد الاختصاص المنصوص عليها في الفقرة الأولى (ب و د) من هذه المادة أو في أي جزء من هذه الفقرات.

و تنص الفقرة 4 من المادة على عدم استبعاد اي اختصاص ينعقد للقضاء الوطني طبقا للقانون المحلي الفقرة 5 تنص على انه في حالة حدوث تنازع في الاختصاص فان يجب ان يتم حله بالتشاور بين الدول الاطراف حول المكان الاكثر ملائمة، كما افردت الاتفاقية بندا خاصا لضرورة التعاون بين الدول.

و لم ينص القانون العربي النموذجي بشان الجرائم المعلوماتية على اي قواعد لتحديد الاختصاص بنظر هذه الجرائم، فان كان الفقه الجنائي اليوم قبل فكرة تطبيق القانون الاجنبي لمواجهة الجريمة عبر الوطنية ما أظهر ضرورة تجاوز فكرة تلازم الاختصاص الجنائي القضائي و التشريعي فيلزم من باب اولى قبول هذه الفكرة و التوسع فيها بالنسبة لجرائم ترتكب في الفضاء الإلكتروني الذي يتجاوز الحدود و القارات، و بذلك نصل الى ضرورة التفكير في وضع ضوابط اسناد جنائية لتحديد الاختصاص الموضوعي و الاجرامي بعد ان تصنف الى فئات مختلفة تشكل كل فئة فكرة مسندة تتضمن المصالح الواجب حمايتها جنائيا على المستوى العالمي لوضع ضوابط اسناد تشير الى القانون الواجب التطبيق[1].

الا أن هذه القواعد يجب ان تتم صياغتها في اطار اتفاقات دولية لأن الجريمة الدولية لا يمكن مواجهتها إلا بالتعاون الدولي، و هو اهم ما جاء في

---

(1) الدكتور جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة 1998م ص 75.

اتفاقيـة بودابسـت بشـكل يسـمح بتبـادل التعـاون سـواء كان ذلـك عـلى مسـتوى جمـع الأدلـة أو تسـليم المجرمـين وهـو مـا يعنـي ان المجتمـع الـدولي مقبـل عـلى توسـع في مجـال التعـاون القضـائي الـذي يتوقـع أن يتـم بـين الاجهـزة القضائيـة، والامنيـة بشـكل مبـاشر نظـراً لأن عامـل الوقـت في حفـظ الادلـة المعلوماتيـة سـوف يكـون حرجـاً ومتطلبـاً لسرعـة الانجـاز[1].

ولعلنـا لا نكـون مغالـين إذا أعطينـا الإختصـاص لاكـثر مـن دولـة، ولكـن الصعوبـة تكمـن في تحديـد أولويـة الإختصـاص عنـد التنـازع، اسـوة بمـا هـو عليـه العمـل في جرائـم التدخـل غـير المـشروع عـلي مـتن الطائـرات للإرتبـاط، والمتمثـل في مـرور وسـيلة النقـل الجـوي بأجـواء أكـثر مـن دولـة.

(1) تدابير مكافحة الجرائم المتصلة بالحواسيب – مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية- المنعقد في بانكوك في الفترة 18-2005/4/25م – وثيقة رقم 14/A/CONF.203.ص 5.

المبحث الثالث

التعاون الدولي

في عـالم تشـغل المعلومـات والبيانـات أهميـة بالغـة سـواء للتبـادل التجـاري، أو للتواصـل الإجتماعـي، مـن مناطـق متباعـدة باسـتخدام تقنيـات لا تكفـل لهـا أمنـا كامـلا، ويتـاح في ظلهـا التلاعـب عـبر الحـدود بتلـك المعطيـات المنقولـة أو المخزنـة، مـما قـد يسـبب لبعـض الـدول أو الأفـراد أو الـشركات أضرارا فادحـة، يغـدو عندهـا التعـاون الـدولي واسـع المـدى في مكافحـة الجرائـم المعلوماتيـة ومـن بينهـا جرائـم الإنترنـت أمـرا محتـما.

ومـع ضرورة هـذا التعـاون، إلا أنـه ثمـة صعوبـات ومعوقـات تقـف دون تحققـه وتجعلـه صعـب المنـال، سـنعرض لأبـرز تلـك الصعوبـات أو المعوقـات، وكيفيـة مواجهتهـا [1].

وسـنوضح ذلك من خـلال المطالب التالية:

المطلـب الأول: الصعوبات التـي تواجه التعاون الدولي.

المطلـب الثـاني: مواجهة الصعوبات التـي تواجه التعاون الدولي.

---

(1) الدكتور جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة 1998م ص 75.

المطلب الأول

الصعوبات التي تواجه التعاون الدولي

حتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول فإنها تحتاج إلى قدرٍ من الأمن والنظام، وتشكل الجريمة إحدى القضايا الرئيسية في الكثير من دول العالم، وتشغل بال الحكومات والمختصين والأفراد على حد سواء، ولقد أثبت الواقع العملي أن الدولة - أي دولة - لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل في كافة ميادين الحياة، فنتيجة للتطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات وظهور الإنترنت والانتشار الواسع والسريع لها أدى إلى ظهور أشكال وأنماط جديدة من الجرائم منها الجرائم المتعلقة بشبكة الإنترنت وهي نوعٌ من الجرائم المعلوماتية، التي باتت تشكل خطرا لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب، بل تعدت إلى أمن البنى الأساسية الحرجة[1].

إلا أنه ثمة صعوبات ومعوقات تقف دون تحقيقه أهمها:

أولا عدم وجود أنموذج موحد للنشاط الإجرامي[2]:

بنظرة متأنية للأنظمة القانونية في التشريعات العربية لمواجهة الجرائم المعلوماتية ومنها الجرائم المتعلقة بشبكة الإنترنت يتضح لنا من خلالها عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم

---

(1) تدابير مكافحة الجرائم المتصلة بالحواسيب - مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية- المنعقد في بانكوك في الفترة 18-2005/4/25م - وثيقة رقم 14/A/CONF.203.

(2) د. عبد الفتاح بيومي حجازي: الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة 2002 ص102

المعلومـات وشـبكة الإنترنـت الواجـب تجريمهـا، فـما يكـون مباحـا في أحـد الأنظمـة قـد يكـون مجرّمـا وغـير مبـاح في نظـام آخـر، ويمكـن إرجـاع ذلـك إلى عـدة أسـباب وعوامـل كاختـلاف البيئـات والعـادات والتقاليـد والديانـات والثقافـات مـن مجتمـع لآخـر، وبالتـالي اختـلاف السياسـة التشريعيـة مـن مجتمـع لآخـر[1].

ثانيـا: تنوع واختلاف النظـم القانونية الإجرائية:

بسـبب تنـوع واختـلاف النظـم القانونيـة الإجرائيـة، نجـد أن طـرق التحـري و التحقيـق و المحاكمـة التـي تثبـت فائدتهـا وفاعليتهـا في دولـة مـا قـد تكـون عديمـة الفائـدة في دولـة أخـرى أو قـد لا يسـمح بإجرائهـا، كـما هـو الحـال بالنسـبة للمراقبـة الإلكترونيـة، والتسـليم المراقـب، والعمليـات المسـتترة، وغيرهـا مـن الإجـراءات الشـبيهة، فـإذا مـا اعتـبرت طريقـة مـا مـن طـرق جمـع الاسـتدلالات أو التحقيـق أنهـا قانونيـة في دولـة معينـة، قـد تكـون ذات الطريقـة غـير مشروعـة في دولـة أخـرى، وبالتـالي فـإن الدولـة الأولى سـوف تشـعر بخيبـة أمـل لعـدم قـدرة سـلطات إنفـاذ القانـون في الدولـة الأخـرى عـلى اسـتخدام مـا تعتـبره هـي أنـه أداة فعّالـة، بالإضافـة إلى أن السـلطات القضائيـة لـدى الدولـة الثانيـة قـد لا تسـمح باسـتخدام أي دليـل إثبـات جـرى الحصـول عليـه بطـرق تـري هـذه الدولـة أنهـا طـرق غـير مشروعـة، حتـى وإن كان هـذا الدليـل تـم الحصـول عليـه بنـاء عـلي اختصـاص قضـائي وبشـكل مـشروع.

ثالثا: عـدم وجود قنوات اتصال:[2]

لعـل التعـاون الـدولي في مجـال مكافحـة الجريمـة والمجرمـين، الحصـول عـلى المعلومـات والبيانـات المتعلقـة بهـم، ولتحقيـق هـذا الهـدف كان لزامـا أن يكـون هنـاك نظـام اتصـال يسـمح للجهـات القائمـة عـلى التحقيـق بالاتصـال بجهـات

(1) د. جميل عبد الباقي الصغير: الجوانب الإجرائية: المرجع السابق ص 72

(2) د. عبدالله محمد صالح الشهري. المعوقات الإدارية في التعامل الأمني مع جرائم الحاسب الآلي: دراسة مسحية على الضباط العاملين بجهاز الأمن العام بمدينة الرياض، رسالة ماجستير غير منشورة، جامعة الملك سعود، الرياض، المملكة العربية السعودية.(1422هـ).

أجنبيـة لجمـع أدلـة معينـة أو معلومـات مهمـة، فعـدم وجـود مثـل هـذا النظـام يعنـي عـدم القـدرة عـلى جمـع الأدلـة والمعلومـات العمليـة التـي غالبـا مـا تكـون مفيـدة في التصـدي لجرائـم معينـة ولمجرمـين معينـين، وبالتـالي تنعـدم الفائـدة مـن هـذا التعـاون.

رابعا: مشـكلة الاختصاص:

الجرائـم المتعلقـة بالإنترنـت مـن أكـبر الجرائـم التـي تثـير مسـألة الاختصـاص عـلى المسـتوى المحـلى أو الـدولي ولا توجـد أي مشـكلة بالنسـبة للاختصـاص عـلى المسـتوى الوطنـي أو المحـلى حيـث يتـم الرجـوع إلى المعايـير المحـددة قانونـا لذلـك[1].

ولكـن المشـكلة تثـار بالنسـبة للاختصـاص عـلى المسـتوى الـدولي حيـث اختـلاف التشريعـات والنظـم القانونيـة والتـي قـد ينجـم عنهـا تنـازع في الاختصـاص بـين الـدول بالنسـبة للجرائـم المتعلقـة بالإنترنـت التـي تتميـز بكونهـا عابـرة للحـدود، فقـد يحـدث أن ترتكـب الجريمـة في إقليـم دولـة معينـة مـن قبـل أجنبـي، فهنـا تكـون الجريمـة خاضعـة للاختصـاص الجنـائي للدولـة الأولى اسـتنادا إلى مبـدأ الإقليميـة[2].

وتخضـع كذلـك لاختصـاص الدولـة الثانيـة عـلى أسـاس مبـدأ الاختصـاص الشـخصي في جانبيـه، وقـد تكـون هـذه الجريمـة مـن الجرائـم التـي تهـدد أمـن وسـلامة دولـة أخـرى فتدخـل عندئـذ في اختصاصهـا اسـتنادا إلى مبـدأ العينيـة[3].

كـما تثـار فكـرة تنـازع الاختصـاص القضـائي في حالـة تأسـيس الاختصـاص عـلى مبـدأ الإقليميـة، كـما لـو قـام الجـاني ببـث الصـور الخليعـة ذات الطابـع الإباحـي

---

(1) هذه المعايير الثلاثة هي مكان القبض على المتهم، مكان وقوع الجريمة أو محل إقامة المتهم

(2) Floret latrive:41 pays contre les pirates.disponible sur:www. liberation.com/multi/actu/2000042420000427/chtml

(3) د. جميل عبد الباقي الصغير: الجوانب الإجرائية، المرجع السابق ص 73

من إقليم دولة معينة وتم الإطلاع عليها في دولة أخرى، ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة[1].

خامسا: التجريم المزدوج:

التجريم المزدوج من أهم الشروط الخاصة للإستجابة لأي طلب لتسليم المجرمين، فهو منصوص عليه في أغلب التشريعات الوطنية والمواثيق الدولية المعنية بتسليم المجرمين، وبالرغم من أهميته تلك[2]، نجده عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية، سيما وأن بعض الدول قد تجرم بعض الأفعال دون تجريم الأفعال التي تتم عن طريق البيئة المعلوماتية، والخاضعة للرقابة والإشراف من قبل مقدمي خدمات الإنترنت، بالإضافة إلى أنه من الصعوبة أن نحدد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم المتعلقة بشبكة الإنترنت أو لا، الأمر الذي يعوق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، ويحول بالتالي دون جمع الأدلة ومحاكمة مرتكبي الجرائم المتعلقة بالإنترنت[3].

(1) www.cybercrime.gov/coepress.html

قبل وضع هذا المشروع كان المجلس الأوربي قد وافق على التوصية رقم 89R-9 وتتضمن هذه التوصية قائمتين بالجرائم التي تقع في مجال الحاسب الآلي، الأولى تحتوى على الحد الأدنى من الجرائم الواجب النص عليها في التشريعات الوطنية للدول المختلفة (ومنها الدخول غير المشروع لنظام الحاسب الآلي أو لشبكة المعلومات)،في حين أن القائمة الثانية اختيارية وتضع مجموعة من الجرائم مثل إتلاف المعلومات وبرامج الحاسب الآلي. للمزيد حول هذه التوصية انظر مقال الدكتور / محمد أبو العلا عقيدة: مواجهة الجرائم الناشئة عن استخدام الحاسب الآلي، مجموعة أعمال مؤتمر حول الكمبيوتر والقانون المنعقدة، بالفيوم من 29 يناير إلي 1 فبراير 1994، ص 119 و120.جامعة عين شمس.

(2) ينص الفصل 40 من مجموعة القانون الجنائي المغربي على ما يلي:«يجوز للمحاكم في الحالات التي يحددها القانون إذا حكمت بعقوبة جنحية أن تحرم المحكوم عليه لمدة تتراوح بين سنة وعشر سنوات، من ممارسة حق أو عدة حقوق من الحقوق الوطنية او المدنية او العائلية المنصوص عليها في الفصل 26. يجوز أيضا للمحاكم تطبيق مقتضيات الفقرة الأولي من هذا الفصل إذا حكمت بعقوبة جنحية من اجل جريمة إرهابية.

(3) الدكتور: جميل عبد الباقي الصغير- الجوانب الإجرائية – المرجع السابق 91

سادسا: المساعدات القضائية:

نعلم أن أول الطرق التي يمكن من خلالها كشف الحقيقة وبخاصة أن الكثير من الدول لا تسمح بالكشف عن الخصوصية المعلوماتية، إلا بإذن قضائي، وبالنسبة لطلبات الإنابة القضائية الدولية والتي تعد من أهم صور المساعدات القضائية الدولية في المجال الجنائي أن تسلم بالطرق الدبلوماسية وهذا بالطبع يجعلها تتسم بالبطء والتعقيد، والذي يتعارض مع طبيعة الإنترنت وما تتميز به من سرعة، وهو الأمر الذي انعكس على الجرائم المتعلقة بالإنترنت[1].

سابعا: التدريب:

تتمثل في عدم الإهتمام من جانب القيادات الإدارية في بعض الدول للتدريب لاعتقادهم بإرتفاع التكلفة، كما أن تطوير العمل من خلال تطبيق ما تعلمه المتدربون في الدورات التدريبية وما اكتسبوه من خبرات لن يعود صداه علي جهات العمل، ومن التي قد تهدد التعاون في مجال التدريب ما يتعلق بالفوارق الفردية بين المتدربين وتأثيرها على عملية الاكتساب للمهارات المستهدفة بقوة تامة و متكافئة لدي مختلف الأفراد المتدربين، سيما في مجال تكنولوجيا المعلومات وشبكات الاتصال حيث أنه يوجد بعض الأشخاص

---

(1) ينص الفصل 26 من مجموعة القانون الجنائي المغربي على ما يلي: (التجريد من الحقوق الرسمية يشمل: عزل المحكوم عليه وطرده من جميع الوظائف وكل الخدمات والأعمال العمومية. حرمان المحكوم عليه من أن يكون ناخبا أو منتخبا وحرمانه بصفة عامة من سائر الحقوق الوطنية ومن حق التحلي بأي وسام. عدم الأهلية للقيام بمهمة محلف أو خبير وعدم الأهلية لأداء الشهادة في أي رسم من الرسوم أو الشهادة أمام القضاء إلا على سبيل الإخبار فقط. عدم أهلية المحكوم عليه بان يكون وصيا أو مشرفا على غير أولاده. الحرمان من حق حمل السلاح ومن الخدمة في الجيش والقيام بالتعليم أو إدارة مدرسة أو العمل في مؤسسة للتعليم كأستاذ أو مدرس أو مراقب. والتجريد من الحقوق الوطنية عندما يكون عقوبة أصلية يحكم به لزجر الجنايات السياسية ولمدة تتراوح بين سنتين وعشر سنوات ما لم تنص مقتضيات خاصة على خلاف ذلك).

ممن لا يعي في هذا المجال شيء، وعلى النظير يوجد أناس على درجة كبيرة من المعرفة والثقافة في هذا المجال[1].

بالإضافة إلى أن الجريمة المعلوماتية تتطور وتحتاج إلي جهات ترصد هذا التطور،، كما ان الجهات المعنية لا تشمل الجهات الشرطية او القضائية، بل تمتد لتشمل كافة القطاعات والأفراد التي تتعامل مع التقنية المعلوماتية - ولاشك أن تفعيل ذلك لا يكون إلا من خلال التدريب المشترك - كما أن كثير من الدول تري ان إستكشاف هذا العالم، بمثابة قدس الأقداس، ومن ثم فهو لا يمس، وبالطبع نسف التعاون الدولي في هذا المجال.[2]

أيضا من الصعوبات التي قد تؤثر على العملية التدريبية وعلى التعاون الدولي فيها ما يتعلق بالملامح العامة المميزة للبيئة التدريبية وعدم قدرتها على تمثيل الواقع العملي لبيئة العمل الطبيعية تمثيلا تاما ومتقنا، من حيث ما يدور بها من وقائع وملابسات وإجراءات، وما يتم فيها من نشاطات لا تبلغ حد التطابق مع طبيعة المهام التي سيؤديها المتدربون في بيئة العمل الطبيعية.

---

(1) ينص الفصل2-218 (يعاقب بالحبس من سنتين إلى ست سنوات وبغرامة تتراوح بين 10000و200000 درهم كل من أشاد بأفعال تكون جريمة إرهابية بواسطة الخطب أو الصياح أو التهديدات المفوه بها في الأماكن أو الاجتماعات العمومية أو بواسطة المكتوبات والمطبوعات المبيعة او الموزعة أو المعروضة للبيع أو المعروضة في الأماكن أو الاجتماعات العمومية أو بواسطة الملصقات المعروضة على أنظار العموم بواسطة مختلف وسائل الإعلام السمعية البصرية والالكترونية).

(2) Office fédéral de la justice، le nouveau media interroge le droit، rapport d un groupe intertemental sur des questions relevant du droit pénal، du droit de la protection des données et du droit d›auteur suscité par Internet،Berne،mai 1996. voir cet article sur le site: www.ofg.admin.ch

انظر في هذا الصدد البحث المقدم من د.محمد أبو العلا عقيدة: الحماية الجنائية للتجارة الالكترونية، ندوة مركز بحوث الشرطة بأكاديمية الشرطة حول المردودات الأمنية لنظام التجارة الالكترونية، أكاديمية الشرطة 29 أبريل2002، ص5. المهندس / حسام شوقى: حماية وأمن المعلومات على الإنترنت، دار الكتب العلمية للنشر والتوزيع، القاهرة، 2003، ص 136.

المطلب الثاني

مواجهة الصعوبات التي تواجه التعاون الدولي

فيما يتعلق بالعقبة الأولي: المتمثلة في عدم وجود نموذج موحد للنشاط الإجرامي فإن الأمر يقتضي توحيد هذه النظم القانونية، ولاستحالة هذا الأمر فإنه لا مناص من البحث عن وسيلة أخرى تساعد على إيجاد تعاون دولي يتفق مع طبيعة هذا النوع المستحدث من الجرائم ويخفف من غلو الفوارق بين الأنظمة العقابية الداخلة، وتتمثل هذه الوسيلة في تحديث التشريعات المحلية المعنية بالجرائم المعلوماتية و إبرام اتفاقيات خاصة يراعي فيها هذا النوع من الجرائم[1]، وان تتم مراجعة لهذه الإتفاقيات بصفة دورية.

وبالنسبة للمعوق الثاني: والخاصة بتنوع واختلاف النظم القانونية الإجرائية نجد أن المواثيق الدولية الصادرة عن الأمم المتحدة غالبا ما تشجع الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة، الشيء الذي يخفف من غلو واختلاف النظم القانونية والإجرائية ويفتح المجال أمام تعاون دولي فعّال.

فمثلا المادة 20 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية تشير في هذا الصدد إلى التسليم المراقب، والمراقبة الإلكترونية وغيرها من أشكال المراقبة والعمليات المستترة[2]، والتي تعتبر من أهم التقنيات

---

(1) من الأمثلة على التشريعات المعنية بالجرائم المعلوماتية: حماية البيانات والخصوصية & القانون الجنائي & حماية الملكية الفكرية & الحماية من المضمون الضار & قانون الإجراءات الجزائية & التشفير والتوثيقات الرقمية. أنظر:

ULRICH SIEBER، Legal Aspects of Computer- Related Crime in the Information Society.Com crime Study. 11998/01/

(2) أنظر أيضا المادة 11 من اتفاقية 1988 بشأن التسليم المراقب & والمادة 50 من اتفاقية الأمم المتحدة لمكافحة الفساد.

المستخدمة في التصدي للجماعات الإجرامية المنظمة، بسبب الأخطار والصعوبات الكامنة وراء محاولة الوصول إلى عملياتها وتجميع المعلومات وأدلة الإثبات لاستخدامها فيما بعد في الملاحقات القضائية المحلية منها أو الدولية في دول أطراف في سياق نظم المساعدة القانونية المتبادلة[1].

وهذا ما أكدت عليه الاتفاقية الأوربية للإجرام المعلوماتي حيث نصت المادة 29 على سرية حفظ البيانات المعلوماتية المخزنة وأجازت لكل طرف أن يطلب من الطرف الآخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل الإلكترونية الموجودة داخل النطاق المكاني لذلك الطرف الآخر والتي ينوي الطرف طالب المساعدة أن يقدم طلباً للمساعدة بشأنها بغرض القيام بالتفتيش أو الدخول بأي طريقة مماثلة، وضبط أو الحصول أو الكشف عن البيانات المشار إليها.

كما أكدت المادة 30 من ذات الاتفاقية على الكشف السريع عن البيانات المحفوظة حيث نصت على: أنه عند تنفيذ طلب حفظ البيانات المتعلقة بالتجارة غير المشروعة والمتعلقة باتصال خاص تطبيقاً لما هو وارد في المادة 29 فإن الطرف المساند إذا اكتشف وجود مؤدي خدمة في بلد آخر قد شارك في نقل هذا الاتصال فإن عليه أن يكشف على وجه السرعة إلى الطرف طالب المساعدة كمية كافية من البيانات المتعلقة بالتجارة غير المشروعة حتى يمكن تحديد هوية مؤدي الخدمة، وهذا الطريق الذي تم الاتصال من خلاله[2].

كما أشارت المادة 31 من هذه الاتفاقية إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة، حيث أجازت لأي طرف أن يطلب من أي طرف آخر

---

(1) راجع في ذلك الأدلة التشريعية لتنفيذ اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبرتوكولات الملحقة بها (منشورات الأمم المتحدة رقم المبيع (E.O.5.V2) الجزء الأول – الفقرة 384.

(2) د/ عبد الكريم غالي: الحماية القانونية للإنسان من مخاطر المعلوميات، رسالة دكتوراة، كلية العلوم القانونية والاقتصادية والاجتماعية، الرباط،1995، ص18

أن يقوم بالتفتيش أو أن يدخل بأي طريقة مشابهة وأن يضبط أو يحصل بطريقة مماثلة، وأن يكشف عن البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكاني لذلك الطرف والتي يدخل فيها أيضاً البيانات المحفوظة وفقاً للمادة 29، ويجب الاستجابة لمثل هذا الطلب بأسرع ما يمكن في الحالات الآتية:

1. إذا كانت هناك أسباب تدعو للاعتقاد أن البيانات المعنية عرضة على وجه الخصوص لمخاطر الفقد أو التعديل.

2. أو أن الوسائل والاتفاقات والتشريعات الواردة في الفقرة 2 تستلزم تعاوناً سريعاً.

في حين نجد أن المادة 32 من ذات الاتفاقية سمحت بالدخول للبيانات المخزنة خارج نطاق الحدود بشرط أن يكون ذلك بموجب اتفاق، أو أن تكون هذه البيانات متاحة للجمهور[1].

أيضا نصت المادة 33 على تعاون الدول الأطراف فيما بينها لجمع البيانات في الوقت الحقيقي عن التجارة غير المشروعة، والمرتبطة باتصالات خاصة على أرضها تتم بواسطة شبكة معلومات، وفي إطار ما هو منصوص عليه في الفقرة الثانية. وينظم هذا التعاون الشروط والإجراءات المنصوص عليها في القانون الداخلي.

ويمنح كل طرف تلك المساعدة على الأقل بالنسبة للجرائم التي يكون جمع المعلومات بشأنها في الوقت الحقيقي متوافر في الأمور المشابهة على المستوى المحلي.

---

(1) GUIDELINES CONCERNING COMPUTERIZED PERSONAL DATA FILES.Adopted by the General Assembly on 14 December 1990:Francesco Miani: le cadre réglementaire des traitements de données personnelles effectues au sein de l›union européenne، revue trimestrielle de droit européen، Dalloz،No.2، 2000، p283

وهنـاك أيضـا المـادة 34 مـن ذات الاتفاقيـة والتـي نصـت عـلى التعـاون في مجـال التقـاط البيانـات المتعلقـة بمضمـون الاتصـالات النوعيـة التـي تتـم عـن طريـق إحـدى شـبكات المعلومـات.

ونلاحـظ مـما سـبق أن: الاتفاقيـة الأوربيـة للإجـرام المعلومـاتي أوجـدت بعـض الحلـول التـي مـن شـأنها التغلـب عـلى مشـكلة اختـلاف النظـم الإجرائيـة أمـام التعـاون الـدولي لمواجهـة الجرائـم المتعلقـة بشـبكة الإنترنـت.

وللحـد مـن ظاهـرة عـدم وجـود قنـوات اتصـال بـين جهـات إنفـاذ القانـون فنلاحـظ أنـه غالبـا مـا تشـجع المواثيـق الدوليـة، الـدول إلى التعـاون فيـما بينهـا وتدعوهـا إلى إنشـاء قنـوات اتصـال بـين سـلطاتها المختصـة ووكالاتهـا ودوائرهـا المتخصصـة بغيـة التيسـير في الحصـول عـلى هـذه المعلومـات وتبادلهـا [1].

ومـن الأمثلـة عـلى هـذه المواثيـق الدوليـة اتفاقيـة الأمـم المتحـدة لمكافحـة الجريمـة المنظمـة عـبر الوطنيـة في المـادة 27 منهـا، والمـادة 9 مـن اتفاقيـة 1988م، والمـادة 48 مـن اتفاقيـة الأمـم المتحـدة لمكافحـة الفسـاد، والبنـد الثـاني مـن المـادة 27 مـن الاتفاقيـة الأوربيـة بشـأن الإجـرام المعلومـاتى، والمـادة 35 مـن ذات الاتفاقيـة الأوربيـة والتـي أوجبـت عـلى الـدول الأطـراف فيهـا ضرورة تحديـد نقطـة اتصـال تعمـل لمـدة 24 سـاعة يوميـاً طـوال أيـام الأسـبوع لـكي تؤمـن المسـاعدة المبـاشرة للتحقيقـات المتعلقـة بجرائـم البيانـات والشـبكات، أو اسـتقبال الأدلـة ذات الشـكل الإلكـتروني، وهـذه المسـاعدة تشـمل تسـهيل أو إذا سـمحت الممارسـات والقوانـين الداخليـة بذلـك، تطبيـق الإجـراءات التاليـة بصفـة مبـاشرة.

أولا: إسـداء النصيحة الفنية.

ثانيـا: حفظ البيانـات وفقاً للمواد 29، 30.

(1) أنظر ما جاء بتوصية المجلس الأوربي رقم R95(13) الصادرة في 1999/09/11م بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات

ثالثا: جمع الأدلة وإعطاء المعلومات ذات الطابع القضائي وتحديد أماكن المشتبه فيهم[1].

كما أوجبت ذات المادة على الدول الأطراف ضرورة أن تتمكن نقطة الاتصال من الاتصال السريع بنقطة اتصال الطرف الآخر، وأن يعمل كل طرف على أن يتوافر لديه الأفراد المدربين القادرين على تسهيل عمل الشبكة.

أما بالنسبة لمشكلة الاختصاص في الجرائم التي تتم عبر الشبكة العنكبوتية فثمة حاجة ملحة إلى إبرام اتفاقيات دولية ثنائية كانت أو جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي خاصة بالنسبة للجرائم المتعلقة بالإنترنت[2]، بالإضافة إلى تحديث القوانين الجنائية الموضوعية منها والإجرائية بما يتناسب والتطور الكبير التي تشهده تكنولوجيا المعلومات والاتصالات.

ولأجل القضاء على مشكلة التجريم المزدوج والذي يعد من أهم الشروط الخاصة بنظام تسليم المجرمين ركزت الاتجاهات والتطورات التشريعية الخاصة بتسليم المجرمين على تخفيف التطبيق الصارم لهذا الشرط، وذلك بإدراج أحكام عامة في المعاهدات والاتفاقيات المعنية بتسليم المجرمين وذلك إما بسرد الأفعال والتي تتطلب أن تجرم كجرائم أو أفعال مخلة بمقتضي قوانين الدولتين معا أو بمجرد السماح بالتسليم لأي سلوك يتم تجريمه ويخضع لمستوى معين من العقوبة في كل دولة[3].

وفيما يتعلق بالصعوبات الخاصة بالمساعدات القضائية الدولية

(1) Charlotte-Marie pitrat-Laurent le veneux: Protection du consommateur et des données personnelles. voir le site: www.finance.gouv.fr،Tierry Leonard: E.Marketing et protection des données à caractère personnel. voir le site: www.droit-technologie.org

(2) علي سبيل المثال 22 من الاتفاقية الأوربية بشأن الإجرام المعلوماتي

(3) د. أسامة عبد الله قايد-الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1988، ص 85.

والتباطؤ في الـرد فإننـا نجـد الحاجـة ملحـة إلى إيجـاد وسـيلة أو طريقـة تتسـم بالسرعـة تسـلم مـن خلالهـا طلبـات الإنابـة كتعـين سـلطة مركزيـة مثـلا أو السـماح بالاتصـال المبـاشر بـين الجهـات المختـص في نظـر مثـل هـذه الطلبـات لنقـضي عـلى مشـكلة البـطء والتعقيـد في تسـليم طلبـات الإنابـة[1]، وهـذا بالفعـل مـا أوصي بـه مؤتمـر الأمـم المتحـدة الحـادي عـشر لمنـع الجريمـة والعدالـة الجنائيـة والـذي انعقـد في بانكـوك في الفـترة مـن 18-2005/4/25م حيـث أكـد عـلى ضرورة تعزيـز فعاليـة السـلطات المركزيـة المعنيـة الضالعـة في أعـمال المسـاعدة القانونيـة المتبادلـة وإقامـة قنـوات مبـاشرة للاتصـال فيـما بينهـا بغيـة ضـمان تنفيـذ الطلبـات في الوقـت المناسـب[2].

ونفـس الـشيء نجـده في البنـد الثـاني مـن المـادة 27 مـن الاتفاقيـة الأوربيـة بشـأن الإجـرام المعلومـاتى، والمـادة35 مـن ذات الاتفاقيـة الأوربيـة والتـي أوجبـت عـلى الـدول الأطـرف فيهـا ضرورة تحديـد نقطـة اتصـال تعمـل لمـدة 24 سـاعة يوميـاً طـوال أيـام الأسـبوع لـكي تؤمـن المسـاعدة المبـاشرة للتحقيقـات المتعلقـة بجرائـم البيانـات والشـبكات، أو الاسـتقبال الأدلـة في الشـكل الإلكـتروني عـن الجرائـم.

كـما أوجبـت ذات المـادة عـلى الـدول الأطـراف ضرورة أن تتمكـن نقطـة الاتصـال مـن الاتصـال السريـع بنقطـة اتصـال الطـرف الآخـر، وأن يعمـل كل طـرف عـلى أن يتوافـر لديـه الأفـراد المدربـين القادريـن عـلى تسـهيل عمـل الشـبكة.

أمـا بالنسـبة للـرد عـلى طلبـات التـماس المسـاعدة فإنـه مـن الـضرورة بمـكان الاسـتجابة الفوريـة والسريعـة عـلى هـذه الطلبـات، لأجـل ذلـك تنـص غالبيـة المعاهـدات والاتفاقيـات الخاصـة بالمسـاعدات القضائيـة المتبادلـة عـلى ضرورة الاسـتجابة الفوريـة والسريعـة عـلى طلبـات التـماس المسـاعدة، وهـذا مـا أكـدت

---

(1) د. مدحت عبد الحليم رمضان- الحماية الجنائية للتجارة الالكترونية،دار النهضة العربية،2001،ط1، ص 77.

(2) تعزيز التعاون الدولي في إنفاذ القانون: مرجع سابق ص 26

عليه الفقرة الثالثة من المادة 25 من الاتفاقية الأوربية للإجرام المعلوماتي حيث نصت على أنه"يمكن لكل طرف، في الحالات الطارئة أن يوجه طلباً للمعاونة أو للاتصالات المتعلقة بها عن طريق وسائل الاتصال السريعة مثل الفاكس أو البريد الإلكتروني على أن تستوفي هذه الوسائل الشروط الكافية المتعلقة بالأمن وصحتها (ويدخل ضمن ذلك الكتابة السرية إذا لزم الأمر) مع تأكيد رسمي لاحق إذا اقتضت الدولة المطلوب منها المساعدة في ذلك. وتقوم الدولة بالموافقة على هذا الطلب والرد عليه عن طريق إحدى وسائل الاتصال السريعة[1].

أما فيما يتعلق بالصعوبات الفنية التي تواجه التعاون الدولي في مجال التدريب فإنه يمكن التغلب عليها بإجراء المزيد من البرامج التي تعمل علي بيان مخاطر الجرائم المعلوماتية والأضرار التي تسببها وبأهمية تدريب رجال العدالة الجزائية على مواجهتها، كما أنه وبمزيد من التنسيق بن الأجهزة المعنية بتدريب رجال تنفيذ القانون إيجاد برامج تدريبية مشتركة تناسب جميع الفئات، كما يتعين الإهتمام بالمساعدين القضائيين، ومنهم رجال الأدلة الجنائيين، وما تم إستحداثه مؤخرا من وظيفة وهي محلل جنائي، وتظهر أهميته في جرائم المعلوماتية.

---

(1) كانت هذه الحماية مثار جدل كبير في فرنسا قبل تدخل المشرع الفرنسي بالنص عليها صراحة القانون رقم 85-660 الصادر في 3 يوليه 1985، وكان الفقه والقضاء هناك منقسمين حول امتداد حماية حق المؤلف إلى برامج الحاسب الآلي بسبب الاختلاف حول توافر شروط المصنف المحمي في برامج الحاسب الالي: انظر على سبيل المثال.

A.Lucas:Les programmes d›ordinateurs comme objets de droits intellectuelles، JCP،1982، 1،Doc، 3081J. Huet: La modification du droit sous l›influence de l informatique، aspect de droitprivé، JCP، 1983،1، Doc، 3095J.L. Goutal: La protection juridique du logiciel،D.1984، Chron، p197 M. Vivant: Informatique et propriété intellectuelle، JCP، 1984، 1 Doc، 3081

وانظر في عرض هذا الخلاف بالتفصيل الدكتور محمد حسام لطفي: الحماية القانونية لبرامج الحاسب الآلي، دار الثقافة للطباعة والنشر،القاهرة 1987 ص 87 وما بعدها.

الخاتمة

اصبح واقعاً ملحاً ضرورة إيلاء النظر إلي المسؤولية الجنائية لمقدمي الخدمات المعلوماتية، وإلي ضرورة التدخل الأمني و التشريعي لتنظيم التعاملات الإليكترونية بصفة عامة، فضلا عن ضرورة وضع أطر تدريبية كفيلة بإستجلاء العلم بالإختراقات الأمنية، وكذا حصر الإعتداءات التي تتم، لأنه لا توجد إحصائيات شاملة لما يحدث فعليا من إعتداءات عبر الشبكة المعلوماتية، قبل اصدار القوانين اللازمة لمواجهة الجرائم المعلوماتية، لأن المعاملات الإليكترونية اليوم أصبحت تغطي معظم التعاملات اليومية، وفي مختلف المجالات، فهي بالتالي ليست جرائم إنترنت بالمعنى الفني وإن كان يطلق عليها الجرائم الإلكترونية إلا انها يمكن ان ترتكب دون استخدام الحاسب الآلي، أما الجرائم المعلوماتية بالمعنى الفني القانوني فهي الجرائم التي لا يتصور ارتكابها دون استخدام التقنية المعلوماتي لأن هذه الأخيرة تشكل عنصراً من عناصرها، مثل الاختراق و تدمير الشبكات و تحريف البيانات أو التلاعب بها و اساءة استخدام بنوك المعلومات.

وقد تعرضت الجريمة المعلوماتية للاعتداء على الحياة الخاصة، حيث افرزت لنا هذه التقنية الحديثة عناصر جديدة للحياة الخاصة لم تعرفها القوانين التي حصرت حمايتها الجنائية فيما تصورت انه يغطي جميع عناصر الحياة الخاصة للإنسان، فقصرت هذه الحماية على المسكن و المحادثات الهاتفية،

دون ان تشـمل تلـك البيانـات المتدفقـة عـبر الشـبكة العنكبوتيـة الدوليـة، وليـس المقصـود هنـا مـا يتـم حفظـه في أرشـيف الدولـة الإلكـتروني، أو تلـك المخزنـة في النظـم المعلوماتيـة للمؤسسـات العامـة، ولكـن الخطـورة تكمـن في مـا يتـم إختزانـه في المؤسسـات الخاصـة وبخاصـة فيـما ينتـج مـن منتديـات أو شـبكات التواصـل الإجتماعيـة التـي تتعامـل مـع الجمهـور مـن جهـة اخـرى، وكثـيراً مـا يتـم الإعتـداء في وقـت يكـون فيـه المتهـم بعيـداً عـن موقـع الجريمـة أو مكانهـا، انتقـل البحـث بعـد ذلـك لتنـاول المشـكلات القانونيـة التـي تثيرهـا الجرائـم المعلوماتيـة مـن حيـث المسـئولية الجنائيـة، بالنسـبة لوسـطاء تشـغيل الشـبكة التـي ترتكـب عـن طريقهـا الجريمـة المعلوماتيـة، فهـذه الأخـيرة يتدخـل لتشـغيلها العديـد مـن الأفـراد أو الجهـات العامـة منهـا و الخاصـة فالشـبكة لا تعمـل الا عـن طريـق مـزود الخدمـة الـذي يمـد العميـل بالوسـيلة الفنيـة التـي توصلـه بالشـبكة، أمـا متعهـد الوصـول فهـو مـن يوفـر لمالـك الموقـع المسـاحة فى الفضـاء الإليكـتروني لـكي يمكنـه مـن اسـتخدامها و تحميلهـا بالمضمـون أو بالبيانـات، وهنـا تثـور اشـكالية حـول امكانيـة تطبيـق الأحـكام العامـة للمسـؤولية الجنائيـة مـما يسـتدعى التدخـل التشريعـي لحسـم هـذه المشـكلة، اذا مـا ارتكبـت عـن طريـق الشـبكة أي مـن جرائـم السـب أو التشـهير، والنظـر إلي البعـد الـدولي للجرائـم المعلوماتيـة موضحـاً أن الجانـب الـدولي لهـذه الجرائـم يشـكل نطاقهـا المـكاني، وليـس عنـصراً فيهـا كـما هـو الحـال بالنسـبة للجريمـة الدوليـة، لأن الجريمـة المعلوماتيـة شـأنها شـأن الجرائـم المنظمـة عـبر الوطنيـة التـي يمكـن ارتكابهـا داخـل حـدود دولـة واحـدة، إلا أن عناصرهـا الماديـة تمتـد لأكـثر مـن دولـة واحـدة، كـما يتعـين إعتبـار جرائـم المعلوماتيـة التـي تتـم عـبر الحـدود جريمـة دوليـة لأن هـذه الأخـيرة، يشـكل العنـصر الـدولي فيهـا عنـصراً مـن عناصرهـا، لذلـك فـإن دراسـة الجانـب الـدولي في هـذه الجرائـم يجـب أن يكـون في محاولـة لتجـاوز القواعـد التقليديـة لتحديـد مبـدأ الاقليميـة الـذي تتأسـس عليـه قواعـد الاختصـاص القضـائي و القانـوني لملاحقـة الجرائـم التـي ترتكـب عـبر أكـثر مـن دولـة.

الإجراءات الوقائية:

1. منع انتحال أرقام الإنترنت أو ما يعرف بـ (Ip-spoofing) والتي يقوم خلالها بعض المتسللين المحترفين باستخدام أرقام بعض الأشخاص بطريقة غير مشروعة، والنص على عقوبة مشددة، حتي ولو كان بإتخاذ برنامج لإخفاء IP.

2. منع إساءة استخدام البريد الإلكتروني أو ما يعرف بـ (E-Mail Spamming) سواء للتهديد أو لإرسال عروض أسعار أو دعايات لا يقبل بها المستخدم وهو ما عرف اصطلاحا باسم البريد المهمل والذي ينتشر بشكل كبير في الدول المتقدمة، وما يتم في الدول العربية من المغالاة في البرامج الدعائية بما يسبب تعطيل للشبكة، دون وجود تنظيم، مستغلين البيانات المخزنة لدي مقدمي خدمات الإنترنت.

3. الاحتفاظ بسجل استخدام مزود الاتصال الخاص بالمشتركين (Dialup-Server) وسجل استخدام البروكسي (Proxy) لمدة لا تقل عن (6) أشهر، عمل رقابة علي مقدمي برامج الكومبيوتر.

4. الحصول على خدمة الوقت (NTP) عن طريق وحدة البروكسي ومزود الاتصال بهدف اللجوء إليها لمعرفة توقيت حدوث عملية الاختراق للأجهزة أو الشبكات.

5. تحديث سجلات منظمة رايب (www.ripe.com) الخاصة بمقدمي الخدمة.

6. ضرورة تنفيذ ما تتوصل إليه وحدات مكافحة جرائم المعلوماتية، وأيا كان مسمياتها علي المستوي العربي أو الدولي، بخصوص متابعة ومعاقبة المخالفات الأمنية، وعمل إستراتيجيات للوقاية من تلك الجرائم.

التوصيات:

1) أهمية تظافر الجهود الدولية من أجل سن القوانين والتشريعات الدولية لمكافحة جرائم الانترنت، وبخاصة النص علي المسؤولية الجنائية المفترضة لوسطاء الخدمة، والزام كافة دول العالم بتطبيق تلك القوانين لضمان القضاء او التخفيف من هذه الجرائم على شبكة الانترنت.

2) حماية صناعة التقنية المعلوماتية والبرمجيات، وذلك لضمان منع عمليات التجسس والقرصنة والاحتيال المالي، وإيلاء متخصصين محترفين لصياغة آليات لهذه المواجهة.

3) تشديد العقوبات المتعلقة بالإرهاب المعلوماتي لما يمثله من خطر داهم على سلامة وامن الوطن والمواطن، وبخاصة المستتر خلف وسطاء مقدمي خدمة الإنترنت.

4) وضع الضوابط التي تمنع الغزو الثقافي المتمثل بالأفكار المنحرفة والمواقع الاباحية التي تستهدف الشباب وتسعى إلى تدميره والتأثير على معتقداته وارادته.

5) اعتبار القرصنة على البرامج بمثابة جريمة مشددة وبخاصة إذا كان الهدف منها إخفاء مرتكب هذه الجرائم، مثلها مثل أي سلعة أخرى.

6) نشر الوعي بأهمية الاستخدام القانوني للبرامج، وإيجاد حلول وقائية فعالة.

7) العمل على إنشاء محاكم للقضايا الافتراضية على شبكة الانترنت لتتمكن من التعامل مع هذه الأنواع المستحدثة من الجرائم، وتدريب جهاز الخدمة المعاونة ومساعدي مأموري الضبط القضائي.

8) التوعية الإعلامية المستمرة للمخاطر الناتجة عن سوء استخدام شبكة الانترنت وما قد تلحقه من أضرار جسيمة على أمن واقتصاد الأوطان والمجتمعات والأفراد.

9) تطوير القدرات التقنية على شبكة الانترنت، وإنشاء شرطة الانترنت للقبض المباشر على مرتكبي الجرائم حال دخولهم على الشبكة من خلال التتبع الفني للجهاز او الخط الهاتفي الذي ارتكبت منه الجريمة.

المراجع

أولاً: المراجع العربية:

1. د. احمد السيد عفيفي – الاحكام العامة للعلانية في قانون العقوبات - دراسة مقارنة 2002– دار النهضة العربية، القاهرة.
2. د. أحمد جلال عز الدين.(1414هـ). أساليب التعاون العربي في مجال التخطيط لمواجهة جرائم الارهاب. الرياض: أكاديمية نايف العربية للعلوم الأمنية.
3. د. أسامة عبد الله قايد – الحماية الجنائية للحياة الخاصة وبنوك المعلومات – دار النهضة العربية القاهرة 1994.
4. د. جميل عبد الباقي الصغير – الانترنت و القانون الجنائي – دار النهضة العربية 2001-.
5. د. حسن صادق المرصفاوي – قانون العقوبات الخاص – منشأة المعارف – الاسكندرية مصر 1991.
6. د. عبد الفتاح بيومي حجازي - جرائم الكمبيوتر والانترنت – في القانون العربي النموذجي دار الكتب القانونية – القاهرة 2007.
7. د. عبد الرحمن محمد بحر.(1420هـ). معوقات التحقيق في جرائم

الإنترنت: دراسة مسحية على ضباط الشرطة في دولة البحرين. رسالة ماجستير غير منشورة، أكاديمية نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية

8. د. عبد الفتاح بيومي حجازي - جرائم الكمبيوتر والانترنت - دار الكتب القانونية القاهرة 2005.

9. د. عبد الله محمد صالح الشهري.(1422هـ). المعوقات الإدارية في التعامل الأمني مع جرائم الحاسب الآلي: دراسة مسحية على الضباط العاملين بجهاز الأمن العام بمدينة الرياض، رسالة ماجستير غير منشورة، جامعة الملك سعود، الرياض، المملكة العربية السعودية.

10. د. فهد بن عبد الله اللحيدان، - الإنترنت، شبكة المعلومات العالمية - الطبعة الأولى- الناشر غير معروف - 1996.

11. د. فتوح الشاذلي - القانون الدولي الجنائي - دار المطبوعات الجامعية - الاسكندرية - 2001.

12. د. كمال أنور محمد القاضي، تطبيق قانون العقوبات من حيث المكان، رسالة

13. دكتوراه، مقدمة إلى كلية الحقوق ـ جامعة القاهرة، 22 إبريل 1965، دار مطابع الشعب

14. د. مبدر سليمان لويس - أثر التطور التكنولوجي مع الحريات الشخصية في النظم السياسية، رسالة الدكتوراة - حقوق القاهرة2005.

15. د. محمد إبراهيم محمد الشافعي، النقود الإلكترونية، مجلة الأمن والحياة، أكاديمية الشرطة، دبي، س 12، ع1، يناير، 2004.

16. د. محمد سامي الشوا ثورة المعلومات وبعكسها على قانون العقوبات دار النهضة العربية القاهرة 1994.

17. د. محمد عبد الطاهر حسين – المسئولية القانونية في مجال شبكات الانترنت - 2002 – دار النهضة العربية – القاهرة.

18. د. محمد حسن منصور – المسؤولون الالكترونين – دار الجامعة، للنشر الاسكندرية 2003.

19. د. محمود نجيب حسني – شرح قانون العقوبات – القسم الخاص – دار النهضة العربية - القاهرة 1986.

20. د. مدحت رمضان – جرائم الاعتداء على الاشخاص و الانترنت – دار النهضة العربية – القاهرة – 2000.

21. الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية، ط 1، 2001

22. د. محمد حسام لطفي - الحماية القانونية لبرامج الحاسب الآلي، دار الثقافة للطباعة والنشر، القاهرة 1987

23. د. ممدوح خليل عمر – حماية الحياة الخاصة والقانون الجنائي – دار النهضة العربية القاهرة 1983.

24. د.منير الجنبيهي – ممدوح الجنبيهي – البنوك الالكترونية ط 2 – 2006 دار الفكر الجامعي – الإسكندرية.

25. د. هلالي عبد الاله احمد.(2000م). تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي. عابدين: النسر الذهبي للطباعة.

26. د. هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1992.

ثانياً: المراجـع الأجنبية:

1. Francesco Miani: le cadre réglementaire des traitements de données personnelles effectues au sein de l'union européenne، revue trimestrielle de droit européen، Dalloz، n2، 2000

2. David Bainbridge- Introduction to computer law-third edition-Pit Man publishing1996

3. Chriss Reed، Internet Law-Cambridge، Universitypress 2004

4. Reuvid، Jonathan. (1998). The Regulation and Prevention of Economic Crime، London: Kogan، 14.

5. Skinner، W. F.، &Fream، A. M. (1997، November).A social learning theory analysis of computer crime among college students. Journal of research in Crime and Delinquency، 34 (4)،

6. Staff.(2000، April2). The Businessof Technology. Available:http:// www. redherring. com/ mag/issue7/ news-security. html [11.10.2001].

7. Thomas، P. (2000، February 23). Insufficient computer security threatens doing business. [Online].

8. Thompson ، R . (1999 ، February) . Chasing after petty

computer crime. IEEE Potentials، 18 (1)، 20 -22.

9. Vacca، John. (1996). Internet Security Secrets.USA: IDG Book. Worldwide Inc.

10. Wilson، c. (2000) Holding management accountable: a new policy for protect against computer crime. Proceedings of the National Aerospace and Electronics Conference، USA 2000، 272281-.

11. ULRICH SIEBER، Legal Aspects of Computer- Related Crime in the Information Society، Com crime Study. 11998/01/

ثالثاً: المراجـع الإلكترونية

1. Adsit، C. Kristin. (1999). Internet Pornography Addiction. [Online].

2. Available: http: // www. chemistry. vt.edu/chem-dept/ dessy/ honors /papers99/adsit. htm [9.3.2001].

3. Highley، Reid. (1999). Viruses: The Internet's Illness.[Online]. Available:http://www.chemistry.vt.edu/chem-dept/dessy/honors / papers99/highleh.htm [9.3.2001].

4. Koerner، B. I. (1999، November 22). Only you can prevent computer intrusions. U.S. News and World Report، 127، pp. 50.

5. Morningstar، Steve. (1998). Internet Crime and

Criminal Procedures.[Online]. Available: http: // www. prevent - abuse - now. com/ index. html [13.10.2001].

6. Nanoart.(2000) [Online]. Available: http://www.nanoart.f2s.com/ hack/ [15.11.2000]

7. . NUA Internet Surveys. (1998، June). How Many Online? [Online]. Available: http: // www. nua. ie/ surveys/ howmayonline/ index.html [26.10.2000].

8. Rapalus، P.(2000، May). Ninety percent of survey respondents detect cyber attacks. Computer Security Institute. [Online]. Available: http://www.gocsi.com/prelen_000321.htm [11.10.2001]

9. Office fédéral de la justice، le nouveau media interroge le droit، rapport d un groupe intertemental sur des questions relevant du droit pénal، du droit de la protection des données et du droit d'auteur suscité par Internet، Berne، mai 1996. voir cet article sur le site: www. ofg.admin.ch

10. GUIDELINES CONCERNING COMPUTERIZED PERSONAL DATA FILES. Adopted by the General Assembly on 14 December 1990 www.un.org

11. Charlotte-Marie pitrat-Laurent le veneux: Protection du consommateur et des données personnelles. voir le site: www.finance. gouv.fr،

12. Tierry Leonard: E.Marketing et protection des données à caractère personnel. voir le site: www.droit-technologie.org

رابعاً: المقالات

1. A.Lucas:Les programmes d'ordinateurs comme objets de droits intellectuelles، JCP، 1982، 1، Doct، 3081

2. J.Huet:La modification du droit sous l'influence de l informatique، aspect de droit privé، JCP، 1983، 1، Doct، 3095

3. J.L.Goutal:La protection juridique du logiciel، D.1984، Chron، p197

4. M.Vivant:Informatique et propriété intellectuelle، JCP، 1984، 1 Doct، 3081

الفهرس